

A Quarterly Journal Devoted to All Aspects of Cryptology

Volume 8 Number 1 January 1984

Cryptology



CRYPTOLOGIA

**A Quarterly Journal Devoted
to All Aspects of Cryptology**

Editors

David Kahn
120 Wooleys Lane
Great Neck, New York 11023

Louis Kruh
17 Alfred Road West
Merrick, New York 11566

Cipher A. Deavours
Department of Mathematics
Kean College of New Jersey
Union, New Jersey 07083

Brian J. Winkel
Division of Mathematics
Rose-Hulman Institute of Technology
Terre Haute, Indiana 47803

Greg Mellen
8441 Morris Circle
Bloomington MN 55437

All correspondence concerning subscriptions, advertising and publications should be sent to the publisher at the Editorial Office, Rose-Hulman Institute of Technology, Terre Haute, Indiana 47803.

See inside back cover for subscription information.

Copyright 1984 as CRYPTOLOGIA at Rose-Hulman Institute of Technology, Terre Haute, Indiana 47803.

ISSN 0161 - 1194.

Manufactured in the United States of America.

Cover: One Danish (Wheatstone) to go! See page 55.

**Assistance of Rose-Hulman Institute of Technology is
acknowledged and appreciated.**

A SYSTEM FOR VERIFYING USER IDENTITY AND AUTHORIZATION AT THE POINT-OF SALE OR ACCESS

GUSTAVUS J. SIMMONS

ABSTRACT: We take for granted that valuable assets and resources, or sensitive and/or high risk facilities, will be physically protected by locks, vaults, alarms, fences, guard forces, etc. Equally important, however, a potential user's identity and authority to use the resource must be verifiable if we are to prevent unauthorized use or access. Elaborate and legally accepted protocols to prevent unauthorized uses are central to all commercial and private transactions. Difficulties arise when the resources are remotely accessible, as in the cases of computer/data files, electronic fund transfers (EFTs), automated bank teller operations, and even in many manned point-of-sale systems. Until recently, no satisfactory counterparts to the established protocols for verifying individual identity and authority had been found. Almost all proposals and systems for achieving this function demand that an individual be able to exhibit a "secret" identifier: a personal identification number (PIN), password, etc. But because such an identifier is transferable, it is not uniquely associated with an individual. We here describe a way to solve this problem, i.e., how to unambiguously identify an individual and to verify his authority to use a resource, using the authentication channel in a novel application of two key cryptography. A personnel identification system using the principles described here—fielded by Sandia National Laboratories in 1980—was the first application of two key cryptography anywhere.

[This work performed at Sandia National Laboratories supported by the U.S. Department of Energy under contract number DE-AC04-76DP00789.]

INTRODUCTION

The class of problems addressed here is well illustrated by remotely accessible computer/data files. Such files may have enormous economic value, because of the value of the information on file and/or the consequences of unauthorized modification of the files. Generally, access to the information in such files and the authorization to modify it requires a password or an identification number to activate a portal. In other words, the requestor's identity and authority are verified through his being able to produce a piece (or more) of information once known to be in the authorized holder's secret possession. Clearly, the system is identifying the key rather than the individual, but, as we shall see there are reasonable scenarios in which the authorized holder of the key may himself desire to defraud the system. Hence, it cannot be assumed a priori that an authorized user is also a trusted participant. Although some element(s) in the system must be trusted, it is possible to transfer this trust from a party that could benefit from its violation either to (1) mechanisms that could only betray the trust through failure or (2) to multiple persons in the expectation that collusion to defraud the system is less probable as the number of persons that must collude is increased.

Basic to all solutions of these problems is some form of authentication, where authentication is interpreted broadly to mean verification that an access request (message) is the utterance of the alleged (authorized) originator and/or that the request has not been altered after its origination. Depending on the specific application, the opponent whose attempted deception the system must detect may variously be (1) an authorized user impersonating other authorized users or illegitimately sharing his right of access with unauthorized persons, (2) the party controlling physical access to the assets or resources or (3) third parties. In many instances, it is required not only that the controller of access be satisfied that the request is authentic, but that in the event of a dispute as to whether an illegitimate use has been made of the assets that the authenticity of the access requests be demonstrable (in a manner both logically compelling and hence eventually legally binding) to an impartial third party or arbiter. Finally, in at least one important class of applications, the information content of the message need not and cannot (by design) be kept secret from those parties who may wish to defeat the system.

Discussed here are three quite different applications of authentication using two key cryptographic techniques that have been made by the Sandia National Laboratories. Each demonstrates an essential part to the solution of the problems described above. The first of these applications--an idealized command and control system--serves as a paradigm for all authentication systems because it encompasses the concerns of both the sender and the

receiver that they be protected from all forms of deception. Unfortunately, the trusted element in such a system may be one of the parties to the exchange, who may (as we have already mentioned) under some circumstances benefit from a compromise of the key that he is supposed to protect. The receiver may falsely attribute a message to the transmitter, or the transmitter may disavow a message that he actually sent, the only evidence being a cipher encrypted using the key that was at one time in the private (secret) possession of both the transmitter and receiver, either of whom could have created the cipher.

The second system to be discussed, partially solves this problem by making the trusted element a tamper-sensitive secure information store that can erase the keying variable if tampering is detected. In addition, for two key cryptosystems the encryption key may be generated—using non-deterministic, random sources—internal to the secure volume and not divulged outside the store, so that it cannot be compromised if the secure information system functions as designed. There are many ways to realize such a secure information store; we have chosen to discuss two systems in which the secure element is physically inaccessible—a borehole seismic package in one case and a surveillance camera in a "hot" reactor area, in the other—to avoid having to digress to discuss the physical technology required to fabricate secure information stores for less malign environments. Given such a secure information store, the problem left unanswered in the command and control system can be partially solved—namely, the receiver can now prove, to his own or an arbiter's satisfaction, that he has received a message processed by the key known to be the transmitter's secure information store. This case still leaves open the question of the integrity of the data being processed, or more generally of the identity of the person using the secure information store. The common proposal to make the secure information store require the user to enter a secret password to be able to use the stored key obviously only moves the original problem from verifying the integrity of one piece of information to verifying the integrity of another.

The third application entails a general technique using two key cryptography for verifying the identity of the person using the store. In this latter system, the trusted element is a physically secure, frequently a multiply manned, identification center at which the identity of individuals is established at the time they are enrolled in the ID verification system. A two key cryptographic system is used as an authentication channel to communicate this verification of identity to remote sites at which the decrypt key is securely stored but where it may be publicly exposed to parties that could benefit from a subversion of the system. The encryption key must of course be kept secret at the central ID facility—perhaps in conventional safes under

two man rule or in shared possession of $h \geq 2$ parties in which $k, h \geq k \geq 2$, of them must cooperate to use the secure information store.

When combined, these three authentication systems make it possible to solve all of the authentication concerns of both the sender and the receiver: the receiver can establish the authenticity of a message in the sense that he can prove that it was generated using the keying variable protected in the secure information store, and since the store can verify the identity of the user, this verification can be communicated over the authentication channel to the receiver who can later prove to an impartial third party that the authenticated order was originated by the individual whose identity has been verified. The transmitter can be certain that the receiver cannot attribute a fraudulent communication to him, and both parties are protected from outsiders (third parties) introducing spurious messages.

THE IDEALIZED COMMAND AND CONTROL PROBLEM

It isn't possible to discuss here actual command and control systems, nor even to abstract many of the subtle problems that characterize such systems. Instead we will discuss an idealized system that is sufficiently broad to cover many military, diplomatic and commercial situations—although we shall describe it in a military-like setting.

Let's posit that a commander has many subordinates whose function it is to execute serious and irreversible acts, such as launching missiles, on receipt of messages containing orders to do so. If the two parties trust each other, then the system at its simplest need only provide authentication to a subordinate that a fire order came from the superior commander. Authentication in this case could be accomplished by including a preagreed upon, but secret from all other parties, message (sign) in the fire order. Since this concern is only that an outsider might impersonate the superior commander and send a spurious fire order, such a naive safeguard would suffice. It could not, however, protect against a third party who intercepted the commander's order to learn the sign and then included it in an altered order to the subordinate in a "postal chess" ploy. Also, it could not prevent one of the subordinates from impersonating the superior commander to another of the subordinates—since they all know the preagreed upon sign. Impersonation is not usually regarded as a significant problem in military command and control situations—but the same sort of deception could be carried out by anyone who learned one of the subordinate's "secret" information. This scenario is often regarded as a significant threat to the system, since the subordinates are normally more exposed than command levels to overrun or capture or to the risk of surreptitious compromise.

The "solutions" to these two problems are related. To prevent a subordinate from impersonating the commander, each subordinate must have an individual sign that the commander uses to authenticate orders. To prevent an outsider from intercepting a communication and stripping off the authenticator and then appending it to a fraudulent order, the communication must be inscrutable to the outsider—technically the message must be block encrypted using a secret key known only to the commander and the subordinate. In an implementation of this scheme using a single key cryptosystem in which the same key is used to encrypt and decrypt, it is still necessary to have individual authenticators if a common key is used, or else individual keys if a common authenticator is used to prevent the bottom-up deception described above.

The command and control system, as described thus far, allows a subordinate to verify the authenticity of an order he acts upon and protects the other subordinates from undetectable forgeries being created from one of the other subordinate's secret information. It provides no protection at all, however, to either the subordinate from his superior disclaiming an order, or to the superior from a subordinate falsely attributing an order to him—since the subordinates could create undetectable forgeries. The insurance against this kind of deception is usually administrative control. In most military authentication systems the subordinate's authenticators are sealed in tamper indicating enclosures—which indelibly indicate that they have been opened. Hence, the subordinate would have to incriminate himself by opening his sealed authenticator, etc.; however, one logical flaw still is that he can claim to have received an order that required the sealed authenticator be opened to determine its authenticity.

Frequently, in very sensitive control situations the superior commander will require a subordinate to verify receipt of an order. In this case, another prearranged message (countersign) from the subordinate would have to be returned. In fact, many military command and control situations are as simple as this. A potential problem remains however: either party could claim to have received the prearranged identifiers when in fact they didn't—equivalent in this case to their being able to generate undetectable forgeries. Because authentication is invariably dependent on recognizing the presence of an already known (or derivable to the authorized users) redundancy in the message, the receiver can only be prevented from making forgeries by denying him the ability to introduce the requisite redundant information into a fraudulent message. This redundancy can be introduced using either one key or two key encryption techniques.

Authentication against deceit by insiders can be achieved using a single key cryptosystem in a simple variation of the common way such systems are used to provide password file security in computer log-in systems. The problem with

an unprotected, i.e., raw, user password file is that anyone having or gaining access to the file could impersonate any user by submitting the user's identifying password. The solution, proposed by Needham [1], is to file not the user's password but a function of the user's password where the function that is exposed in the computer is noninvertible or "one way." Any secure cryptosystem can be used as a one way function to provide the desired password file protection. In a single key cryptosystem, the cipher (message) can be found given the key and message (cipher), whereas the key cannot be recovered from a knowledge of the cipher and message (known plain-text attack); hence, a one way function exists between the key and the message/cipher pair. In password file protection, the user's password is therefore the key and the message is some fixed test phrase that is encrypted with each user's key into the cipher stored in the file. Anyone having access to the encryption algorithm, the test phrase and the cipher file would still be unable to impersonate a user, while a user can reliably authenticate himself by presenting the key that encrypts the test phrase to a cipher matching his stored cipher.

One way to use this idea in the present command and control example would be for the commander to select a message and a key with which he computes a test cipher. He then gives the test cipher and message to his subordinate but keeps the key secret to himself. When the superior wishes to issue an authenticated order he sends his key as an authenticator. The subordinate decrypts the test cipher and matches the messages to verify the authenticity of the order. He can later prove that he received the order from his superior since he can exhibit the key that he could have obtained only by either receiving it from his superior commander as arranged or else by breaking the cryptosystem to recover the key from the known plaintext and the test cipher. The return acknowledgement could be handled in a similar fashion.

Even though demonstrable (by the receiver) that authentication has been provided, there are still possibilities for deceit. Unless the original exchange of test cipher and message is witnessed and securely stored by a third party, either party could later generate a key and cipher pair matching a fraudulent message and assert that these are the true pair and that the key was received from the other party as authentication for a communication, or conversely, disavow a true pair as fraudulent or as having been generated ex post facto. A third party or arbiter in this case would be unable to resolve either of the possible disputes.

Much more serious, though, in the scheme just described is the limitation that it is possible to communicate only an authenticated signal to execute some already agreed-to plan; in other words the key can be revealed (or used) only once. If two or more messages were known to be authenticated by the same key, the receiver could substitute any one of these messages for the order that he

actually received, because the authenticator proves only that the superior commander has sent one of the messages—not that he sent a particular message. A one time authenticator is, in a sense, message independent.

By prearranging a large number of battle plans and ciphers (i.e., by enlarging the code book), an execute signal could be authenticated for any particular plan by the superior commander revealing the appropriate key. However, it should be obvious that, for even a modest number of options (orders) and of subordinates, the amount of information that must be exchanged in advance of the need to communicate has grown enormously. Each subordinate requires at least a unique key and a code book—or in the most extreme case, a unique code book. Thus, while (in principle) our idealized command and control problem can be solved using one key cryptosystems, in practice, a full solution of the sort just described is impractical.

The crucial difference between one key and two key cryptosystems in simple message authentication is that it is possible in the latter to avoid the need to distribute the random entry code book in advance! In the direct analog to the authentication system just described, the existence of the two keys, d and e , that act as functional inverses to each other in a two key cryptosystem makes it possible for the transmitter to compute a cipher using e , that will decrypt into an acceptable message using d . Therefore, the receiver and arbiter could each be given the decryption key, d , and a succinct (functional) description of the identifying redundant information that must be in authentic messages. For example, all acceptable messages might end in a time, date and message number. Since e is concealed from a knowledge of d by a computationally infeasible task, the receiver—even though he knows the form of all acceptable messages—has no better chance of constructing a cipher that will decrypt into such a message than does a third party who must guess at ciphers. The transmitter, on the other hand, authenticates messages simply by being in possession of a key with which he can generate ciphers that decrypt into acceptable messages.

It is also possible in a two key cryptosystem to give the receiver and the arbiter the decryption key in advance and then to authenticate a message by presenting a message/cipher pair in which the cipher will decrypt using the receiver's key to the message. This is in fact the way that one of the first two key authentication systems developed at the Sandia National Laboratories operated.

The bottom line to this discussion is that the command and control system just described appears to allow the receiver to authenticate a message as having come from the authorized transmitter and to later prove the authenticity of this order to a third party. At the same time it protects a transmitter from

having a fraudulent order attributed to him by one of the receivers. Superficially, it appears that the command and control problem has been completely solved—without identifying a trusted element in the system. This is not the case, however. The encryption key, e , must be kept secret by the transmitter just as in the single key case. In the sign/countersign type of system described earlier, there had to be two encryption keys: one used by the commander to authenticate (sign) his orders to the subordinate and one used by the subordinate to authenticate his responses or queries to command. In either direction of communication there is a logical flaw. For example, the subordinate cannot "prove" the authenticity of an order if the superior commander's key was either compromised or claimed to have been compromised by the superior commander. Again, this is normally not considered a real problem in command and control applications because of discipline and administrative controls that are feasible at centralized headquarters for command. This sort of administrative control is harder to provide for the dispersed and exposed subordinate commands and of course virtually impossible to provide in a commercial or private exchange setting. In either case, though, this loophole represents a conceptual flaw in the system just described [2]. Later we shall show how the systems described in the following two sections can be combined to avoid even this problem.

SECURE INFORMATION (KEY) STORES IN AUTHENTICATION

Probably the most unique class of authentication problems solved to date at the Sandia National Laboratories are characterized by requiring message authentication while at the same time not permitting concealment of the message from opponents who may wish to defeat the system. These problems first arose in the late 1960's in the design of systems to verify international compliance with treaties limiting arms production or testing. Since that time several other problems of the same generic type have arisen, e.g., the IAEA (International Atomic Energy Agency) RECOVER system that monitors power reactors worldwide to control fissile materials. In all of these applications, a collection of sensors is to be emplaced in a physically secure, but unattended, installation to collect data that would with high confidence reveal noncompliance with the terms of a treaty or licensing agreement. For example, TV cameras installed in "hot" cells of a power reactor to permit IAEA monitoring of fuel rods, unattended seismic installations emplaced in a host nation to detect underground nuclear testing or activity monitors on a heavy armament production line, etc. This data must then be transmitted to the monitor (receiver) over a public communications channel. From the viewpoint of the monitor, an opponent, usually assumed to be the host for the sensor emplacement but possibly a third party desiring to undermine the treaty arrangements, may either modify incriminating messages to innocuous ones or else introduce

spurious incriminating messages to mislead the monitor into erroneously reporting violations. This latter tactic is especially significant when only a negotiated, but limited, number of on-site verification inspections are permitted the monitor. Obviously (again from the monitor's viewpoint), the probability of having either an altered or counterfeit message be accepted as authentic can be made as small as desired by block encrypting the data from the sensors along with a sufficient number of message identifiers, such as time, date, message number, etc., prior to transmission. This encrypting is accomplished, however, at the expense of concealing the content of the message from the host. Such secrecy is generally intolerable to the host (and perhaps to third parties) since the monitor could then cheat on the terms of the agreement by transmitting information concealed in the cipher other than that agreed to. In other words, for such a system to be acceptable, the plaintext message consisting of the output of the sensors as well as the identifying information must be legible to the host at least—and perhaps to specified third parties. Conversely, for the system to be acceptable to the monitor this exposure of the message content should not increase the probability of an opponent, whether the host or a third party, being able to cause a modified or substitute message to be accepted as authentic.

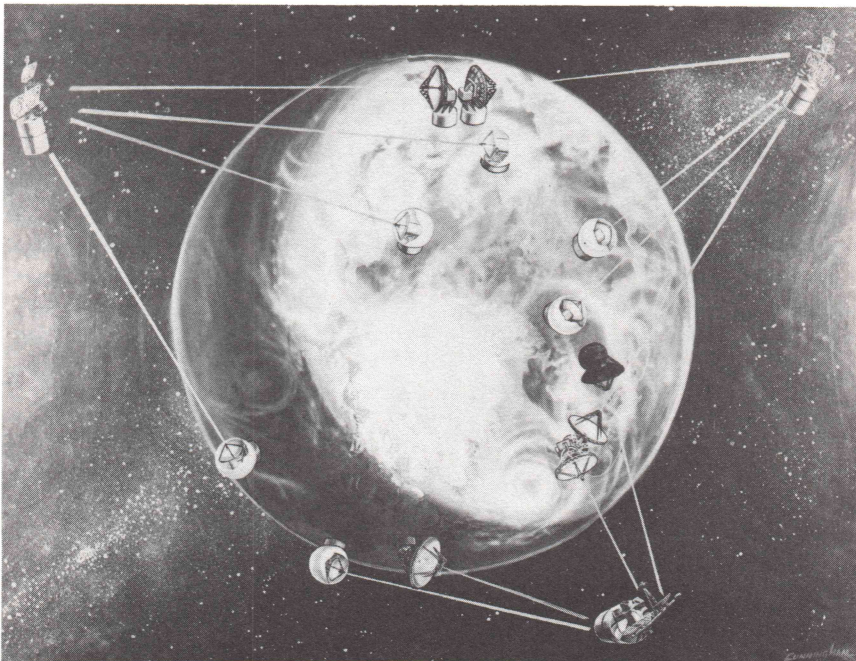


Figure 1. Artist's Rendering of World Wide NSS Data Network.

Even if both of these objectives are realized, there is still another subtle aspect to these problems. If the action to be taken by the monitor in the event that a violation of the treaty or agreement is detected involves third parties or arbiters--such as the United Nations, IAEA, NATO, The World Bank, etc.--then it must also be impossible for the monitor to forge messages. Otherwise, the host to the sensors could disavow an incriminating message as having been fabricated by the monitor, an assertion which the monitor could not disprove if it were within his capabilities to create an undetectable forgery. Recalling the discussion in the previous section of the various types of deception that authentication detects, it should be clear that a solution in the present case requires the encryption key to be protected from all parties, i.e., unknown and kept secret from all of them.

The first system for message authentication without secrecy, using only a single key cryptosystem, has been described extensively elsewhere, Figures 1 and 2 [3,4]. It required a compromise on the monitor's part of the quality of authentication achieved and on the host's part as to the amount of information that was temporarily inscrutable to him. For the purposes of this paper, we describe two two-key cryptosystem solutions, both of which use the Rivest-Shamir-Adleman (RSA) algorithm. Readers unfamiliar with this algorithm can find explanations in any of several good references [3,5,6].

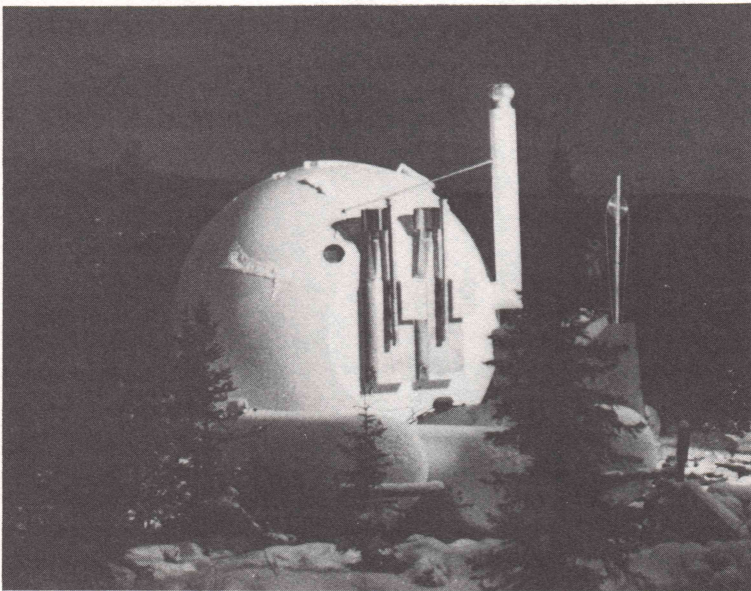


Figure 2. Alaskan NSS Station.

The simplest possible implementation of an authentication system without secrecy using a two key encryption algorithm resolves some of the compromises inherent in a single key encryption algorithm based systems. In a two key scheme the monitor chooses the primes p and q and one of the encryption exponents (keys) e or d , then calculates the inverse exponent (key) d or e , respectively. As part of the initialization procedure by the monitor, $n = pq$, and e would be securely entered either into the down-hole seismic package or the fuel rod placement monitor (the secure elements in these systems). The seismic sensors, Figure 3, would detect any attempt to gain physical access to the package long before the information security is in jeopardy. In the fuel rod placement monitor developed by Sandia and emplaced at the Canadian Chalk River Reactor for test and evaluation, the high radiation levels in the "hot" cell provided the general tamper resistance—and a relatively unsophisticated tamper resistant stressed glass container was adequate to insure against tampering by remote manipulators. It is this tamper sensitive storage volume that characterizes a secure information store. The point is that in both of these applications the environment makes it easy to believe that the "secure information store" will detect tampering before the integrity of the stored keys is jeopardized. A viable and demonstrable technology has been developed, primarily at the Sandia National Laboratories, for fabricating secure information stores for less malign environments; however a discussion of this technology is inappropriate to our purposes here.

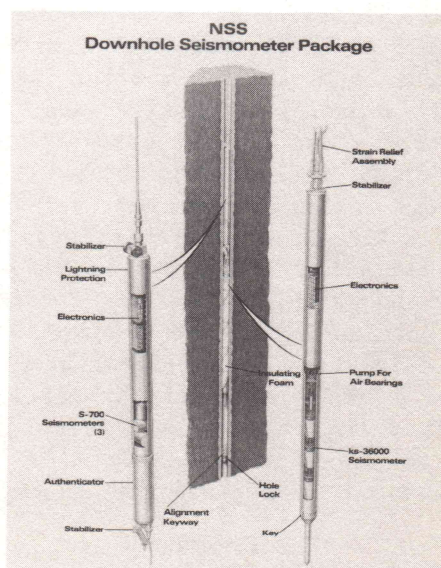


Figure 3. NSS Down-hole Seismometer Package.

Returning to the discussion of the seismic data authentication system, the decryption key, d and n , would be given to the host—and of course retained by the monitor. In operation, the seismic data as well as the redundant identifying information would be block encrypted using the key e and n . The host could decrypt in real time, even delaying transmission in a buffer until decryption was completed, to reassure himself that no unauthorized (to the monitor) information was concealed in the message. He is assumed to know the actual seismic data (message) either from his own sensors or from data links to the monitor's sensors ahead of the authentication operation. The monitor, on the other hand, can be certain of the authenticity of a message (containing message numbers, clock readout, etc.) since by hypothesis neither the host nor any third party can compute e from the exposed n and d . Thus the host need not trust the monitor at all, while the monitor is free to introduce as much redundant (but preknown to the host) information as he wishes to provide authentication confidence. This system fails in exactly the same way that the one based on one key techniques did when a third party must be convinced that a violation has been detected. Since the monitor still has the capability of generating undetectable forgeries, the host can claim the message is a forgery created by the monitor to embarrass him and the monitor cannot prove otherwise.

Even this problem can be solved. As noted earlier, clearly, no party can be in possession of e , since they could then (by definition) generate undetectable forgeries. Since there are no scenarios in which the objectives of the monitor and of the host are furthered by their collaborating to create undetectable forgeries, it might at first seem that a solution would be to split the knowledge of e between the host and the monitor in such a way that neither alone could recover e . For example, the monitor and host might each enter an n -bit random binary number, R_m and R_h , respectively, and their exclusive OR (mod 2) sum taken as e . Neither the host nor the monitor could infer anything about e from their knowledge of the random component they had selected, hence neither would be able to utter an undetectable forgery. The host, however, could still defeat the functioning of the system in the following way: He could test with impunity, and when incriminating records are exhibited by the monitor claim that his copy of R_h has been compromised (e.g., one of his people has defected, his files have been rifled, etc.) The point is that he can either deliberately or inadvertantly make it possible for the monitor to have recovered e and hence to generate undetectable forgeries, etc., as before. The host could therefore unilaterally make it impossible for the monitor to prove to an unbiased third party that the monitor did not create a forgery.

The solution is for the equipment in the secure element of the system to generate p and q in secret from all parties and then to select e (also in secret from all parties), revealing only n and d which it calculates using p , q and e . The decryption key, n and d would be output at the end of the initialization process to the monitor, to the host and to any arbiters needed. In such a system, only the equipment in the secure information store, which is physically secure, could generate ciphers that would be accepted as authentic message—and unlike the various compromise systems described above, all of the objectives of each of the parties are completely realized:

1. No party is able to forge messages that would be accepted as authentic.
2. All parties, i.e., host, monitor and third parties are able to independently verify the authenticity of messages.
3. No unilateral action possible on the part of any party can lessen the confidence of any party about the authenticity of messages.
4. No part of the message is concealed from the host or from specified third parties.

The essential point of a system design for message authentication without secrecy is that a secure information store that can detect tampering and initiate the rapid volatilization of the stored key is the trusted element. In fact, Glenn R. Norris and I designed several tamper sensing secure information stores in the mid-60s for precisely such applications. Unfortunately, this particular tamper sensing technology is still classified; however, functionally similar technologies are described in open literature. The important point, though, is that a tamper detecting container can be used as the trusted element in an authentication system so that no party can gain access to the key and create undetectable forgeries. There is still one lingering flaw to this concept: the container identifies only itself—or more precisely, the secret key that it contains—not the integrity of the data it processes nor the identity of the party using it. This isn't a problem for either the seismic sensor package or for the fuel rod placement monitor, since the environment precludes anyone feeding false information to these systems—but it would be a problem for application to the command and control problem discussed in the preceding section and even more so for commercial applications where the secure information stores would be exposed to a large and varying audience of users (and abusers). The next section discusses a means for solving this problem.

INDIVIDUAL CERTIFICATION

At the close of the section on the idealized command and control system, we noted that the receiver could prove only that an order (message) had been generated using the key belong to the transmitter—but not that the authorized transmitter had originated the message. In the immediately preceding section we discussed a means of mechanistically insuring the secrecy of the encryption key using secure information stores, but for the remote access or automated-use situation in which an individual is responsible for originating the communication, this scheme still left in doubt the identity of the party using the key to encrypt messages. In various guises this failure characterizes all individual identification systems which equate identity with the possession of a piece of information that was once known to be in either the private possession of the individual identified or in a tamper sensing secure information store. In this section we describe a means of associating an individual with an unforgeable piece of information using two key cryptographic systems in such a way that it is feasible to verify the association whenever the individual needs to be identified. Consequently, the bearer can be identified (associated) with the information and the problem described above solved.

The function of the authentication system to be described here is to identify an individual by his unique attributes using only reference materials that he has in his possession. There is the additional restriction that very little communication to other sites be required in advance of, and none at the time that the individual's identity is to be verified. Finally, there is the practical constraint—arising from multi-site dispersal of the receivers or access controllers, as well as both the number of persons and the turn-over in staff having access to the access control at the site—that while information at the site must be protected from alteration or substitution, it is generally not possible to guarantee its secrecy. It is this ability at the remote location to protect the integrity of—but not keep secret—the decrypt key that is the crucial trusted element in such a system. This will typically be accomplished by some sort of tamper sensing container with the key being entered publicly—often jointly by two or more persons. In a point of sale system for example, the store manager and the chief teller might each enter keys in the morning and verify their correctness by decrypting known test ciphers. For the system to function, it is essential that the correct key be used, hence, to be protected from modification or replacement. Secrecy is not needed however.

The solution is so simple as to be almost anti-climactic. A central facility is entrusted by all of the parties (sites) needing to verify individual's identities, to first establish the identity to whatever degree of certainty deemed necessary and then to generate an ID record for each individual

identified. This record will comprise personal attributes (photograph, fingerprints, hand geometry, voiceprint, retinal prints, signature, etc.) encrypted using the encrypt key of a two key system along with descriptive identifiers such as name, social security number, etc. System function is totally dependent on the central site's keeping the encrypt key secret, i.e., making the secure element actually secure. Depending on the application, this system may require two (or more) man rule for access or k out of n shared key reconstructions to require an improbably high level of collusion for subversion to be possible. The decrypt key would be delivered as an authenticated, but not necessarily secret, message to the sites who would have to protect the integrity but not the privacy of the key. When, at some later time, an individual appears at a site with a claimed identity, he would present the cipher record in his possession and permit his individual attributes to be reread by equipment at the site. Using the decrypt key, the site would first decrypt the ID cipher and verify the authenticity of the cipher by the presence of the expected redundant information. They would next check for a suitable agreement between the individual attributes just measured by equipment located at the site and the decrypted attributes contained in the authenticated message. If a match is achieved, the identity of the individual has been confirmed since the cipher could only have been generated using the secret encrypt key held by the enrollment station which was responsible for establishing the identity of the individual. The only advance communication required between the site and central facility is the authenticated (but not necessarily secret) exchange of the decrypt key. For example, what has come to be known as the "Merkle channel" can be used in which the key is communicated over so many public channels — newspapers, television, radio, etc. — that it would be infeasible for an opponent to usurp all, or even most, of them. The other channel of communication is the public one of the user bringing his own ID cipher to the site. Since authentication is possible in a two key cryptosystem in which the sender's key is known to be secure, the site can be certain (to the same level as the two key cryptosystem is cryptosecure) that the ID records it has received are authentic, i.e., issued by the central authority. Then, to the degree that the information in the ID records can identify an individual, the remote users can be confident of the identification. No communication with the central facility is required at the time that the individual is identified, and more importantly, no files of identifying information for possible users need be transmitted to and stored at the site! The crucial point is that the separation of the encryption and the decryption capabilities in a two key cryptosystems has been exploited to devolve the authentication capability from the sender to the receiver—and hence has transferred the ability to determine the veracity of the ID records supplied by the applicant to the receiver (site). The fact about two key cryptosystems on which this concept depends is that it is possible to transfer the ability to authenticate (messages) over an authentication channel.

The first application of the principles described here and indeed the first application of a two key cryptographic system revealed in the open literature was in an access control system designed by the Sandia National Laboratories and successfully installed by the Sandia Safeguards Development Department and operated at the Idaho National Engineering Laboratory, Idaho [7]. This system, designated as a Positive Personnel Identity Verification (PPIV) device, Figure 4, is an optional subsystem supplementary to the international nuclear material containment portal used by the International Atomic Energy Agency (IAEA) to prevent the unauthorized removal of nuclear materials from a facility.

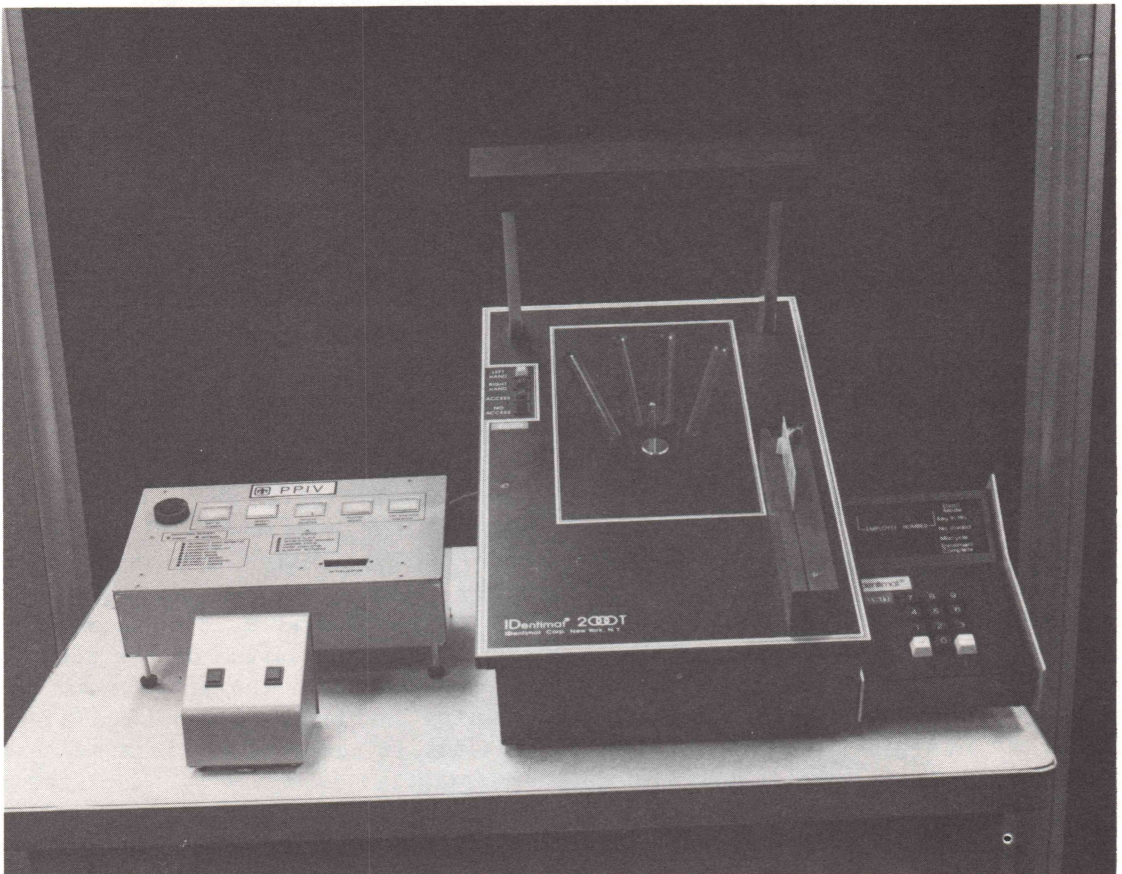


Figure 4. PPIV Entry Station.

The international portal is automated so that a human operator is not required to be in attendance during normal operation and is a stand alone unit so far as its data processing is concerned; without links to a central computer or

data bank. For direct compatibility, the PPIV was designed to operate in the same manner. The individual attribute chosen for corroboration of identity was hand geometry. The measurements are made on commercially available equipment, the IDentimat 2000T manufactured by the IDentimat Corp. of New York, Figure 5.

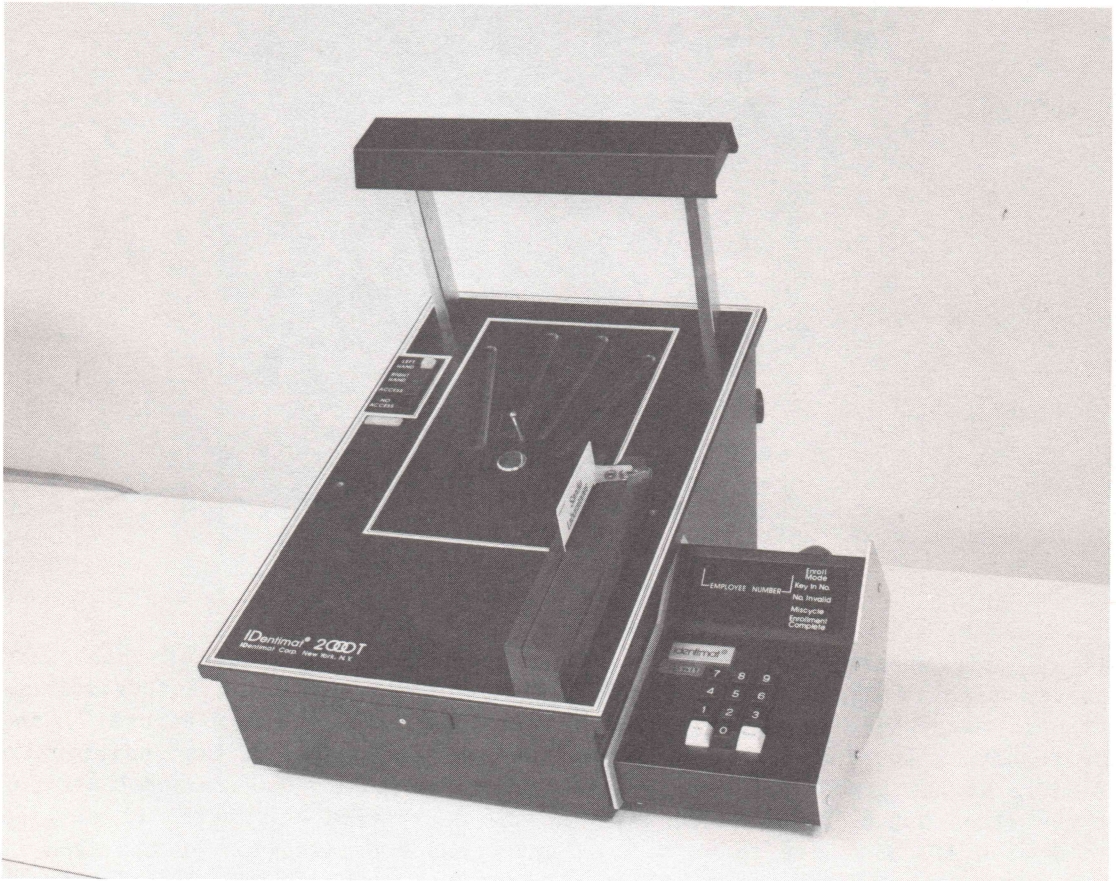


Figure 5. Hand Geometry Reader Used in PPIV.

To make it difficult for more than one subject to be certified and authorized entry bases on a single identity and authority verification, the individual's weight is part of the ID record—and the weight of the occupant(s) of the booth is read by sensors in the access portal. For added security, a user is required to enter a five-digit, random but private, memorized ID number, Figure 6.

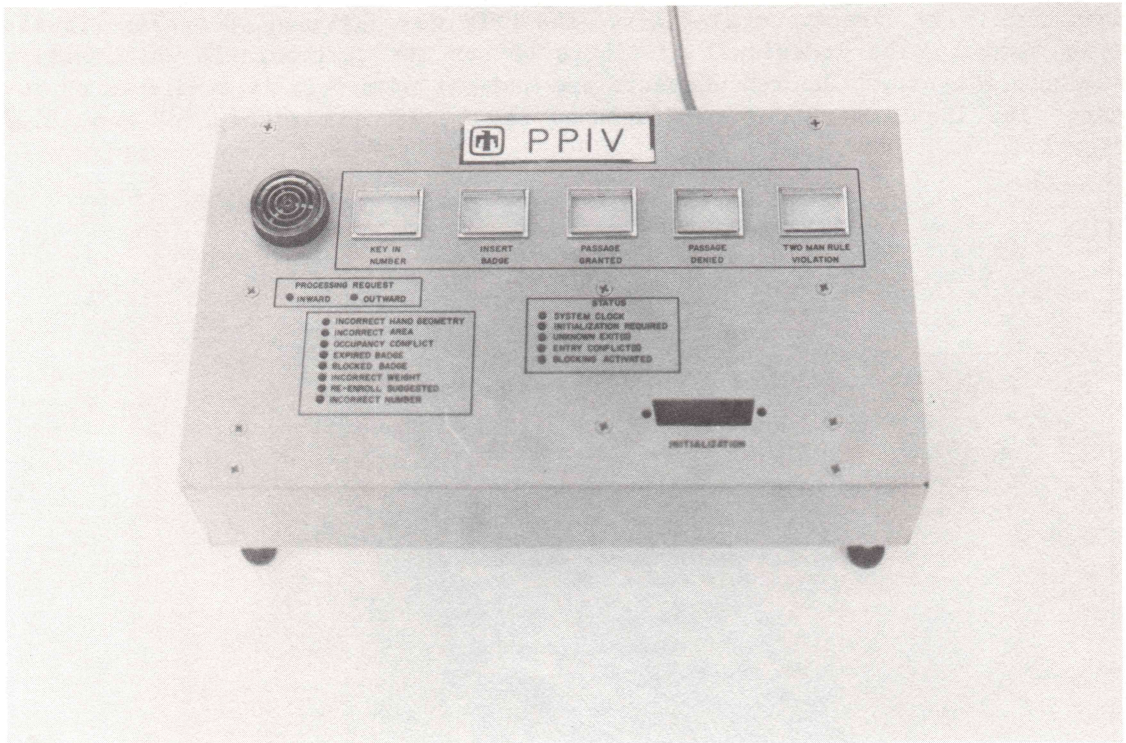


Figure 6. PPIV Controller.

All of this information, along with data defining the areas of authorized access, time of day in which access is authorized, period of authorization, etc., is encrypted using the Rivest-Shamir-Adleman algorithm, Figure 7, and the resulting ID cipher is recorded on a magnetic stripe on the individual's ID badge at the time he is enrolled in the system. The access control station at the site must be initialized with the RSA decryption key, date, time, list of blocked IDs that are to be refused entry and a designation of the area it controls—so that it can correctly respond to the area authorization in the ID ciphers.

The first system has been operational for three years. A second, expanded system has since been installed at a fuel rod reprocessing facility. The reliability of the identification is precisely that claimed for hand geometry verification by IDentimat (in the 90% region), but the underlying principle is independent of the particular choice of the attribute to be measured. Several other commercially available automatic identity verification devices are available and have been extensively tested in the Air Force Base and Installation Security System (BISS) program: an automatic fingerprint verification

(AFV) system by Calspan Corp., Buffalo, New York; an automatic speaker verification (ASV) system by Texas Instruments, Dallas, Texas; and an Automatic Handwriting Verification (AHV) system by Veripen, Inc., of New York. In addition, Sandia National Laboratories has developed a dynamic signature verification system that is compatible with many identity verification applications.

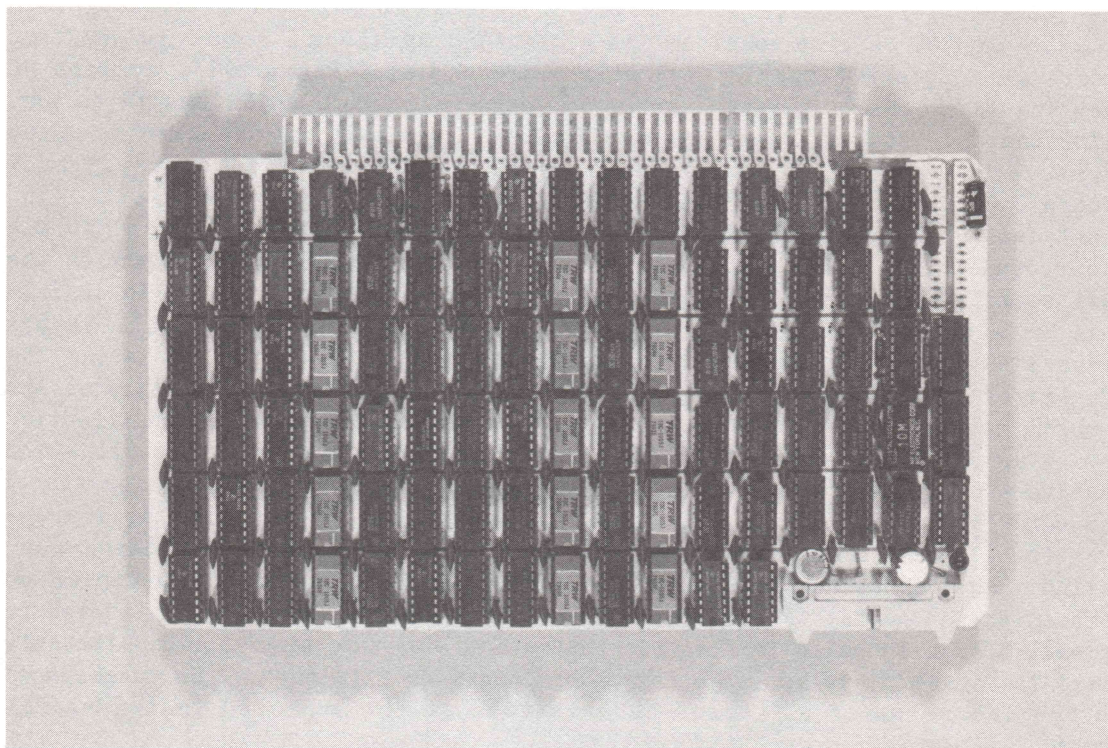


Figure 7. RSA Cryptoboard for PPIV.

The bottom line to this discussion is that equipment exists to measure various individual attributes to implement the identification technique described before. The first reduction to practice by the Sandia National Laboratories in the PPIV, using hand geometry measurements, illustrates the general principle.

CONCLUSION

In a two key cryptographic system, it is possible for a receiver to authenticate a message as having been encrypted using the authorized transmitter's key. The receiver can therefore authenticate the message as having been sent by the authorized transmitter to the same level of confidence that he has that the transmitter's key has been kept secret. The problem is that if insuring the secrecy of the key is the responsibility of an individual, it may be in his interest (if he wants to deceive the system) to either deliberately compromise the key or else to claim its probable compromise. Secure information stores that detect tampering and volatilize a stored key provide a means of insuring the secrecy of a key generated inside the store and known to no one. Unfortunately, such a secure information store can only authenticate messages as having been processed by the store--but cannot (when used simply as a secure information store) verify the identity of the party using it. The usual device of requiring the insertion of an access code or password to use the store is subject to precisely the same type of failure described in the last section: i.e., it equates the verification of the identity of an individual with the possession of a piece of information once known to be in his private possession. However, the secure information store can, by using the identity verification techniques just described, establish the identity of the user through an authenticated message from a central identity verification facility. In other words, these two subsystems used in conjunction allow the receiver to authenticate messages as coming from the secure information store, and also allow the secure information store to verify and communicate the identity of the user. There are still problems, such as a user being compelled under duress to misuse the system. It is unrealistic to expect an authentication system to be able to detect this type of deception--although it is easy enough to build in features that allow the user to either undetectably alert the system that he is acting under duress or else to lock up in response to the insertion of a "scram" code instead of the expected individual ID number.

In summary, the authentication systems described here, based on several different uses of two key cryptography, illustrate all of the elements required for user identification and remote-authentication messages as would be needed in even the most sensitive commercial applications.

REFERENCES

1. Needham, R.M. and M.D. Schroeder. 1978. Using encryption for authentication in large networks of computers. Comm. ACM. 21: 993-999.
2. Simmons, G.J. 1980. Secure communications in the presence of pervasive deceit. Proceedings of the 1980 Symposium on Security and Privacy. 84-93.
3. Simmons, G.J. 1979. Symmetric and asymmetric encryption. Computing Surveys. 11: 305-330.
4. Simmons, G.J. 1981. Message authentication without secrecy. In Secure Communications and Asymmetric Cryptosystems, edited by G.J. Simmons, AAAS Selected Symposia Series. Boulder CO: Westview Press, 105-139.
5. Rivest, R., A. Shamir and L. Adleman. 1978. A method for obtaining digital signatures and public-key cryptosystems. Comm. ACM. 21: 120-126.
6. Knuth, D.E. 1981. Seminumerical Algorithms: The Art of Computer Programming. Vol. 2, 2nd Ed., Chap. 4. Reading MA: Addison-Wesley Pub. Co.
7. Merillat, P.D. 1979. Secure stand-alone positive personnel identity verification system (SSA-PPIV). Sandia National Laboratories Tech. Rpt. SAND79-0070 (March).



Reprinted by permission. Copyright NEA, Inc.

LUCIFER, A CRYPTOGRAPHIC ALGORITHM

ARTHUR SORKIN

ABSTRACT: Lucifer, a direct predecessor of the DES algorithm, is a block-cipher having a 128 bit block size and 128 bit key length. Its general design principles and properties are described and discussed. A simple FORTRAN program is presented which implements the algorithm, providing a modern, secure cryptographic algorithm that can be used in personal computers. Lucifer is of special interest because it is in the same class of product ciphers as DES but is much simpler. Study of Lucifer may reveal cryptanalytic methods that can be applied to DES.

KEYWORDS: Lucifer, block ciphers, DES, cryptographic algorithms, FORTRAN programs.

I. Introduction

Lucifer is a high security, 128 bit key, block-cipher algorithm with a 128 bit block size. It is a direct predecessor of DES and is the same variety of product cipher, using alternating linear and non-linear transformations. Lucifer is therefore a good subject for cryptanalysis in order to discover principles that can be applied to DES.

One of the principle complaints about DES is the short, 56 bit length of the key. It is asserted [4,5] that DES could be broken by exhaustive search at a reasonable cost with today's hardware. It is also asserted that by 1990, the increased speed of the available hardware will make DES so insecure that some form of replacement will be a necessity [4]. It is unlikely that exhaustive search will ever be a feasible technique with Lucifer because of its 128 bit key length, and it is extremely likely that any successor of DES will have a 128 bit key [4].

DES has also been criticized because some of its design principles have been kept secret at the request of NSA [11,12], allowing for the possibility that there are weaknesses that only NSA and its designers are aware of. The same degree of secrecy does not appear to have been applied to Lucifer.

Because of its relationship to DES, and its relative simplicity compared to DES, Lucifer is worthy of study. An understanding of Lucifer helps to clarify the internal operation of DES, since the principal elements of Lucifer are also present in DES, though in more complex form. Since Lucifer and DES have similar key-message statistical properties, and Lucifer is very resistant to exhaustive search because of its 128 bit key, Lucifer appears to be relatively strong cryptographically. Lucifer's relative simplicity also makes it an extremely easy algorithm to implement in software, making it a reasonable candidate for use on a personal computer.

This paper discusses the development of Lucifer, its design and hardware implementation. The relationship of Lucifer to DES is also discussed, and some suggestions for cryptanalytic study are made. An original FORTRAN implementation is presented that is suitable for use on a personal computer or in other applications.

II. The Hardware Device

Lucifer was developed at IBM Thomas J. Watson Research Laboratory in the early 1970's [6,16] and was the subject of several U.S. patents [7,8,9,17]. The original Lucifer was a prototype cryptographic device constructed at Watson Laboratory for use in data communication. The Lucifer device was combined with the IBM 2770 Data Communications System as part of an experiment in computer security. A software algorithm provided the same cryptographic transformation in the host computer. The Lucifer device allowed the key to be loaded at the operator's option either from ROM or from magnetic cards. A mode selection switch allowed three modes of operation. One mode disabled the cryptographic function, and, therefore, cleartext was both sent and received. A second mode enabled Lucifer to receive ciphertext and decipher it; messages received in cleartext were not altered. Cleartext was always transmitted. The third mode was similar to the second, except that, in addition, all messages transmitted were enciphered.

The Lucifer device was constructed from standard TTL SSI and TTL MSI components. In all, 178 TTL modules were used, mounted on four wire-wrap boards. The state-of-the-art in LSI at the time Lucifer was constructed had an influence on the design of the device (and therefore the algorithm) in that an attempt was made to limit the complexity of the circuits. As a result, the Lucifer hardware used circular shift registers to store the key and the two halves of the message in order to simplify access to successive bytes. The APL program written by IBM that implements the algorithm in software mimics

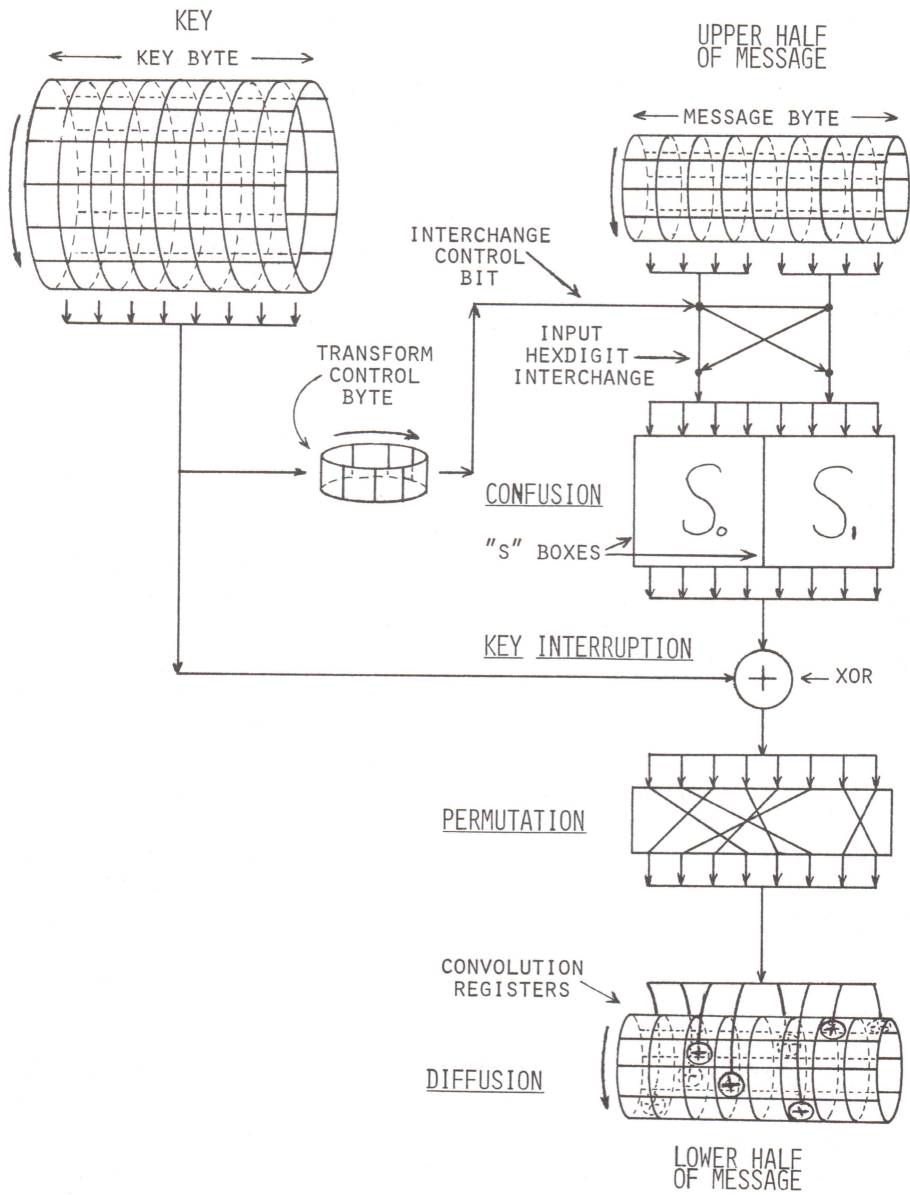


Figure 1. Block Diagram of CID logic.

the hardware by actually shifting the key and halves of the message. The Fortran programs, discussed in Section V and shown in the Appendices, do not move the key or halves of the message; the appropriate bytes are accessed in place as needed.

III. The Algorithm

The Lucifer algorithm is a product cipher that uses alternating linear and non-linear transformations with the choice of non-linear transformation under control of the key [6,16]. Informally, a linear transformation, T , on a vector space, V , is one that has the linearity property: $T(ax+by) = aT(x)+bT(y)$, where x and y are vectors and a and b are scalars. A non-linear transformation is one that does not have the linearity property. Strings of bits and Boolean operations can form a vector space with bit strings vectors, individual bits scalars, bitwise EXCLUSIVE-OR vector addition, and bitwise logical AND multiplication by a scalar. For a formal treatment see [11,14]. For example, a permutation $p(x_1x_2 \dots x_n) = x_{p(1)}x_{p(2)} \dots x_{p(n)}$ of a string of bits is a linear transformation.

Lucifer has a block size and key size of 128 bits (16 bytes). 128 bit plaintext blocks produce 128 bit ciphertext blocks under control of the 128 bit key. Every bit of the key and every bit of the cleartext participate in the construction of every bit of the ciphertext. Tests conducted by IBM indicate that the change of a single bit in either the key or the message causes approximately half (64) of the bits in the resulting ciphertext to change [16]. The probability that a particular ciphertext bit will change appears to be very close to one-half, and the probabilities seem to be independent for each bit of the ciphertext block.

The message block to be enciphered is divided into two halves, the upper and lower, each containing eight bytes (64 bits). The bytes of the message are initially ordered so that the rightmost byte is the highest, and the leftmost byte is the lowest. Encryption (and decryption) is divided into sixteen rounds. A block diagram of the functional units appearing in one round is shown in Figure 1. During a round, the lower half of the message is transformed; the upper half is not changed, but its contents are used as input to the transformation. Between rounds, the upper and lower halves of the message are exchanged.

The sixteen bytes of the key and the eight bytes of each message half can be viewed as being enscribed axially on the face of three cylinders. The cylinders all rotate in the same direction. Let the initial position of byte zero on each cylinder be the origin for that cylinder with respect to rotation

along its axis. The rotation of each cylinder by one step brings a new byte to the origin. The number of the new byte is one greater (modulo 16) than the number of the previous byte.

		MESSAGE BYTE							
		0	1	2	3	4	5	6	7
C-I-D ROUND	1	0	1	2	3	4	5	6	7
	2	7	8	9	10	11	12	13	14
	3	14	15	0	1	2	3	4	5
	4	5	6	7	8	9	10	11	12
	5	12	13	14	15	0	1	2	3
	6	3	4	5	6	7	8	9	10
	7	10	11	12	13	14	15	0	1
	8	1	2	3	4	5	6	7	8
	9	8	9	10	11	12	13	14	15
	10	15	0	1	2	3	4	5	6
	11	6	7	8	9	10	11	12	13
	12	13	14	15	0	1	2	3	4
	13	4	5	6	7	8	9	10	11
	14	11	12	13	14	15	0	1	2
	15	2	3	4	5	6	7	8	9
	16	9	10	11	12	13	14	15	0

Figure 2. Key byte access schedule.

The halves of the message move in step and rotate one position after each byte is used. Byte zero returns to the origin on both cylinders after eight steps, i.e. one round. During encryption, the key rotates one step after each key byte is used, except at the end of each round, when it does not advance.

Therefore, the key byte that ended the previous round begins the next one. For example, bytes zero through seven are used in the first round, and byte seven, not zero, starts the second round. For decryption, the key bytes are accessed in reverse order. The key is initially rotated to bring byte eight to the origin. Before each round and after each byte is used, the key advances one step. Thus, the first decryption round starts with byte nine and rotates past byte fifteen to end with byte zero; byte two starts the second round. Different key bytes are accessed in each round; the period of repetition is sixteen, so after the last round, the key is back in its initial position. The order in which the key bytes are accessed for each round is shown in Figure 2 and is discussed further in Section IV. The rotation of the key is not in step with the rotation of the two halves of the message. This permits the bits of every key byte to be used in the generation of every ciphertext bit.

The first key byte accessed in each round is used as the transform-control-byte. Its number is the leftmost entry in each row (round) in Figure 2. Each of its eight bits in turn becomes the interchange-control-bit, which is used to choose which of two non-linear transformations will be applied to a byte in the upper half of the message. For both encryption and decryption, bits seven through zero of the transform-control-byte choose the transform for bytes zero through seven of the upper half of the message respectively.

The non-linear transformations contain two different non-linear substitution boxes (S-boxes), S_0 and S_1 . Each S-box has four input bits and four output bits, so the input and output can represent the numbers from zero to fifteen (one hexdigit) in binary. An S-box can be considered to implement a permutation of the numbers from 0 to 15. Equivalently, it can also be viewed as a simple substitution of 4-bit quantities into 4-bit quantities. The Lucifer S-box implementation decodes the four binary bits into values from zero to fifteen, performs a fixed permutation of the values from zero to fifteen, and encodes the values from zero to fifteen back into four binary bits. While the internal S-box permutation is a linear transformation of the 4 input bits when they are considered to be binary numbers from 0 to 15, it is a non-linear transformation of the four input bits when they are considered to be simply a vector of bits. A block diagram of an S-box appears in Figure 3. The permutations for S_0 and S_1 are shown in Figure 4. If the interchange-control-bit is zero, then the right hexdigit of the message byte is input to S_1 and the left hexdigit is input to S_0 . If the interchange-control-bit is one, then the hexdigit inputs to the S-boxes are interchanged; the right hexdigit is input to S_0 and the left hexdigit is input to S_1 . One of two non-linear transforms results. The generation of transformed bytes using the bytes of the upper half of the message as input to the key-controlled S-boxes is called confusion.

S-BOX IMPLEMENTATION

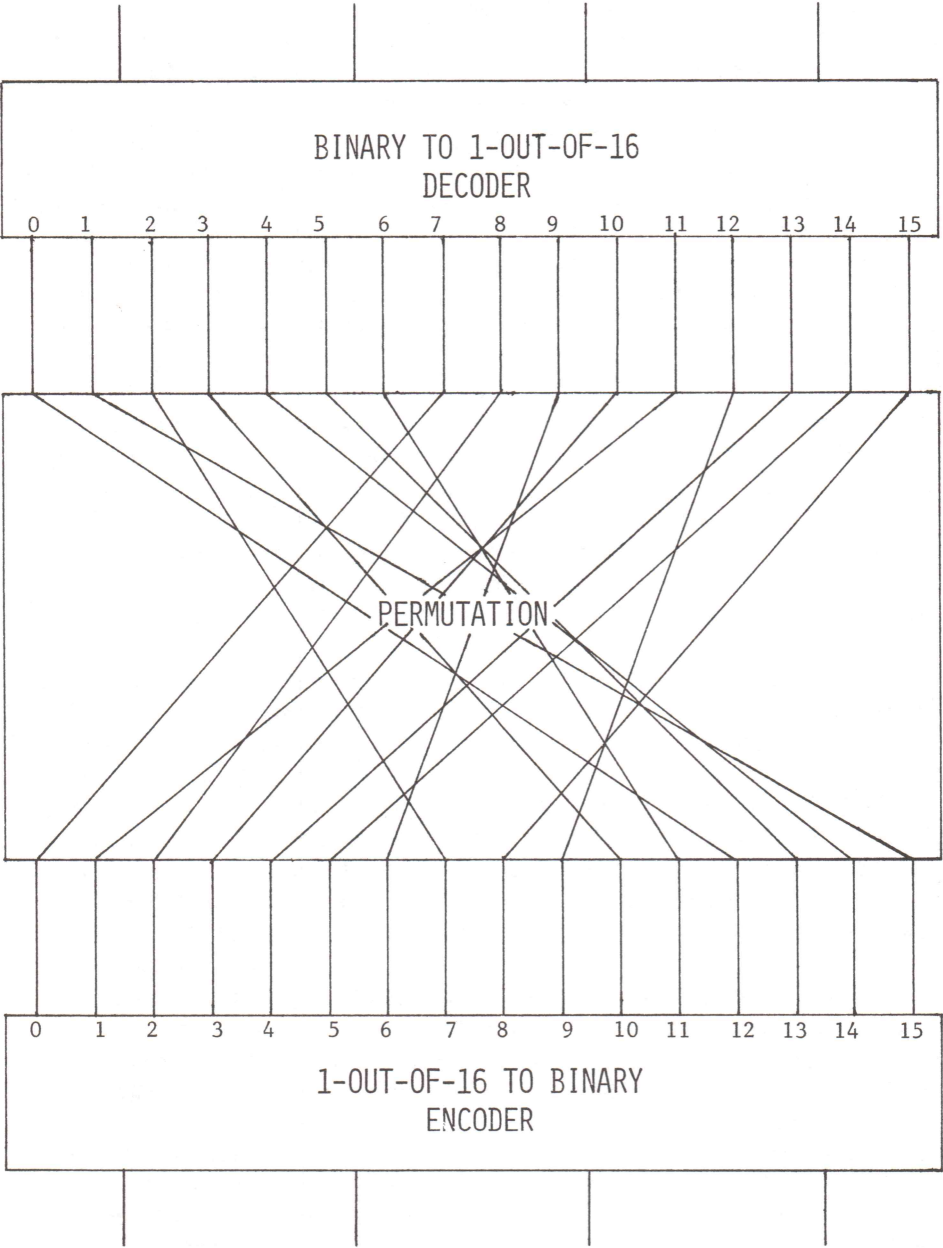


Figure 3.

S-BOX INTERNAL PERMUTATIONS			
S ₀		S ₁	
0 ---- 12		0 ----- 7	FIXED PERMUTATION
1 ---- 15		1 ----- 2	
2 ----- 7		2 ---- 14	
3 ---- 10		3 ----- 9	
4 ---- 14		4 ----- 3	
5 ---- 13		5 ---- 11	
6 ---- 11		6 ----- 0	
7 ----- 0		7 ----- 4	
8 ----- 2		8 ---- 12	0 ---- 3
9 ----- 6		9 ---- 13	1 ---- 5
10 ----- 3		10 ----- 1	2 ---- 0
11 ----- 1		11 ---- 10	3 ---- 4
12 ----- 9		12 ----- 6	4 ---- 2
13 ----- 4		13 ---- 15	5 ---- 1
14 ----- 5		14 ----- 8	6 ---- 7
15 ----- 8		15 ----- 5	7 ---- 6

Figure 4. Permutations.

For step *n* in a particular round, a confused byte is generated from byte *n* in the upper message half. It is then bitwise XOR'ed (addition modulo 2) with the key byte that is at the origin of the key cylinder for step *n* in that particular round. Figure 2 shows the key byte accessed for every step of each round. This process is called key interruption, since the use of the key acts as a barrier to cryptanalysis by merging some secret information into the confused bytes. The eight bits of each resulting interrupted byte are permuted according to a fixed permutation, shown in Figures 1 and 4.

The permuted bits are then XOR'ed with eight bits of the lower part of the message. The eight bits in the lower half of the message are chosen according to the bit pattern of convolution XOR cells shown in Figures 1 and 5. The convolution XOR cells remain fixed in space with respect to the origin as the lower message cylinder rotates. Figure 5 shows the lower message cylinder and convolution cells of Figure 1 cut at the origin and unfolded. As the cylinder rotates, each permuted-interrupted byte is bitwise XOR'ed with a different eight bits of the lower half of the message. All 64 bits of the lower message

PATTERN OF XOR CELLS

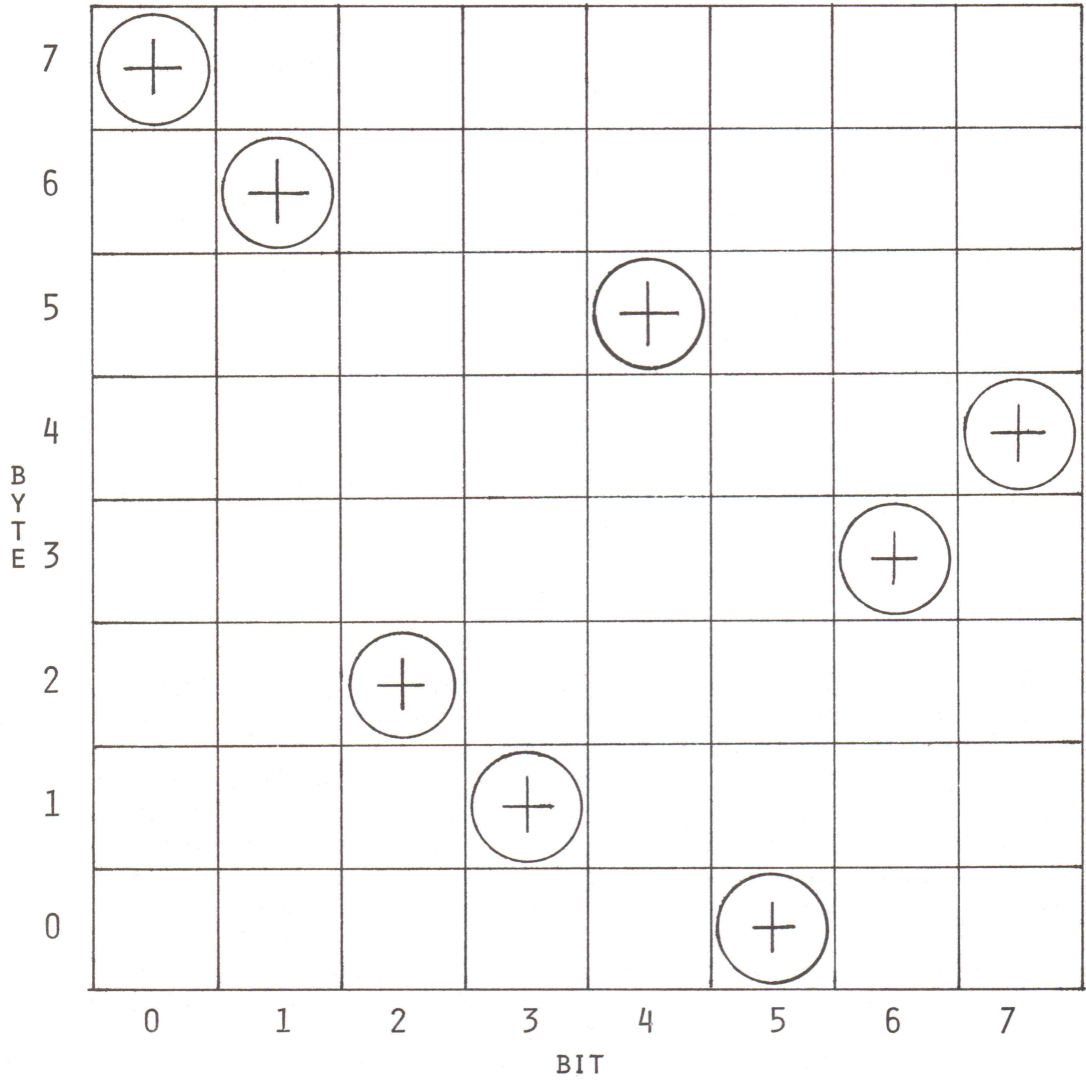


Figure 5. Unfolded convolution registers.

half are used in each round, and each bit is used exactly once. This process is called diffusion, since the result of the transformation of one-half of the message is diffused throughout the other half of the message. Key-interruption and diffusion can be combined because XOR is associative and commutative.

The confusion, key interruption, and diffusion (c-i-d) cycle described above forms a single round. Confusion and diffusion were first suggested as a way in which to create a cryptographically strong cipher by Shannon in his well-known paper on secrecy systems [15]. Confusion, key interruption and diffusion are also used in DES, though in a somewhat more complex manner than in Lucifer [13]. The description of DES is actually more understandable when looked upon as describing key interruption, confusion, and then diffusion.

The Lucifer c-i-d cycle is repeated sixteen times with fifteen interchanges of the upper and lower message halves. The result is the ciphertext. Deciphering is performed by repeating the c-i-d cycles in reverse order, with the key rotated eight positions before the beginning of the first decryption round. In the sixteen repetitions of the c-i-d cycle, each of the 128 key bits is used once for confusion control and eight times for key interruption, so every bit of the ciphertext depends in a very complex way upon every bit of the message and every bit of the key.

IV. Key-Byte Access Schedule

Figure 2 shows the order in which the key bytes (rows) are accessed for each round. Each entry in the table is the number of the key byte to be accessed. For encipher operations the key bytes are taken from left to right and top to bottom. For decipher operations the key bytes are taken from left to right and bottom to top. The leftmost column contains the number of the transform-control-byte. The rows show the numbers of the eight key bytes used for key-interruption in the corresponding round. Each element of row $n + 1$ of the table is obtained by adding 7 modulo 16 to the corresponding element of row n . Alternatively, each element of row n is obtained by adding 9 modulo 16 ($= -7$ modulo 16) to the corresponding element of row $n + 1$. In implementing the algorithm, it is not necessary to store the key-byte access schedule in tabular form, since it merely shows the exact order in which the key bytes pass the origin during the rotation of the key, as described above.

V. FORTRAN Programs

The original IBM report describing Lucifer contains an APL implementation that

emulates the hardware implementation. A FORTRAN implementation was developed for this paper because APL is very hard to read and understand, and APL is unavailable on most small and many large computers. In addition, APL can be quite inefficient. On the other hand, FORTRAN is very widely available (including on personal computers), FORTRAN has an ANSI Standard, and FORTRAN programs are usually compiled so they normally have reasonable performance. The FORTRAN implementation was developed by comparing the APL program with the hardware block diagrams and written descriptions contained in [6,16]. There were some ambiguities in the written description of the order in which the bits of the key and message were loaded and stored in the hardware. These ambiguities were resolved by reference to the APL implementation.

Appendix 1 presents a simple FORTRAN subroutine which implements Lucifer. Because very few high-level languages, including FORTRAN, are well suited for bit manipulation operations, the message and key are stored in integer arrays with one message or key bit per array element; the value of each array element must be either zero or one. The subroutine assumes that the key and message have already been converted from input format into array format by another subroutine; no attempt is made to verify that every array element is either zero or one.

The subroutine handles the key and message halves in place, without rotating them. Instead, pointers are used to indicate which key and message bytes are to be accessed, and the pointers are moved instead. The message is stored in variable *m* as an 8x8x2 three dimensional array (column, row, plane). It can be equivalenced to a 128 element one dimensional array. The planes correspond to the two halves of the message. The key is stored in the variable *k* as a 16 x 8 two dimensional array (column, row). It can be equivalenced to a 128 element one dimensional array. Variables *s0* and *s1* contain the permutations for the S-boxes, and variable *pr* contains the inverse of the fixed permutation used after key interruption. If the variable *d* is equal to one, then the subroutine deciphers; otherwise, it enciphers. Variable *jj* contains the index of the message byte (row) being accessed; variable *kk* contains the index of the bit (column) being accessed. Variable *p(0)* contains the index of the lower half of the message; *p(1)* contains the index of the upper half of the message. Variable *kc* holds the array index of the key byte currently being accessed; *ks* holds the array index of the transform-control-byte. Lines 7600 through 10000 implement the S-boxes and interchange control. Lines 10200 through 10900 implement key interruption and diffusion. Key interruption and diffusion are combined into one operation by first permuting the confused byte and the key byte, and then doing the XOR's (implemented as addition modulo 2). The diffusion pattern is contained in variable *o*, and the convolution cell for column *kk* and row *jj* is equal to $(o(kk)+jj) \bmod 8$. Because the subroutine operates on the message in place, it is necessary to physically swap the

contents of the upper and lower halves after the end of the sixteen rounds in order to have the halves in the correct order. Lines 10900 through 11900 implement the interchange. This final swap would not have been necessary if we have been physically swapping halves all along.

Appendix 2 presents a sample FORTRAN program which calls Lucifer. The message block is enciphered and deciphered 500 times each, so that Lucifer is invoked 1000 times. Appendix 3 shows the timing for 1000 invocations. On a VAX 11/780 computer, the time to encrypt or decrypt a 128 bit block is approximately 100 ms. On the same computer, an NBS supplied version of the DES algorithm [13] takes between 40 and 50 ms to encrypt or decrypt 64 bits. It should be possible to speed up the Lucifer subroutine by optimizing it, however, that was not done in this presentation for reasons of clarity. An optimized program would not have corresponded in an obvious way to the description and figures presented in the rest of the paper.

Appendix 4 shows a subroutine that expands input bytes into array format, and a subroutine that compresses array format back into byte format. The conversion from byte format to array format guarantees that each array element is either one or zero.

VI. Conclusion

A recent article [3] asked if there was a reasonably secure, modern cryptographic algorithm that could be easily implemented on a personal computer. The FORTRAN version of the Lucifer algorithm presented in this paper is very suitable for use on a personal computer. The advantages of FORTRAN are that it is widely available, standardized, and usually produces programs with reasonable performance. The Lucifer FORTRAN implementation is simple and reasonably fast. These programs can be optimized for speed, though the particular techniques employed would depend upon the processor used and its architecture. The programs presented here can easily be converted into another programming language (e.g. BASIC).

Lucifer is also interesting because it is the direct predecessor of DES, but is much simpler than DES. For example, Lucifer only has two S-boxes, the minimum possible for this kind of product cipher with rotating key, and therefore, the key is used to choose between the same two non-linear transforms in every round. DES effectively has 32 S-boxes (constructed from 8 more complicated ones), and the choice of which non-linear transforms are used in each round depends upon input bits as well as key bits. [13] Studying the properties of Lucifer should yield some insights into the cryptanalysis of product cipher with rotating keys.

It is known that without the rotating key this type of cipher is weak [10]. Some statistical techniques have been developed that allow cryptanalysis under a known-plaintext attack of very simple ciphers using alternating S-boxes and permutations [1,2]. It is possible that these techniques might be extended to Lucifer and DES, and they need not provide a complete cryptanalysis. The statistical attack might be used in combination with exhaustive search by first reducing the set of possible keys to a practical size; exhaustive search would then be used to examine every remaining key to find the correct one. However, to-date, the only publicly known cryptanalysis of Lucifer or DES is exhaustive search of the entire key space, which is currently impractical for DES and virtually impossible for Lucifer [4,5,11,12].

Even if the combined statistical/brute-force method suggested in the previous paragraph doesn't work, understanding the simpler Lucifer problem should help us to understand the DES problem, which, in turn, might lead to cryptanalytic techniques that can be applied directly to DES. Also, understanding the ways in which Lucifer was strengthened (to arrive at DES) might aid us in understanding the (still classified) criteria used by IBM (and NSA) to design and evaluate DES. This in turn might answer some of the questions raised about the existence of hidden weaknesses in DES.

VII. Acknowledgements

This work was performed under the auspices of the U. S. Department of Energy by Lawrence Livermore National Laboratory under contract number W-7405-ENG-48.

REFERENCES

1. Andelman, D. 1979. Maximum Likelihood Estimation Applied to Cryptanalysis, Doctoral Dissertation, Stanford University, Department of Electrical Engineering. December.
2. Andelman, D., and J. Reed. 1982. On the Cryptanalysis of Rotor Machines and Substitution-Permutation Networks. IEEE Transactions on Information Theory. 28: 578-584.
3. Deavours, C. A. 1982. The Black Chamber. Cryptologia. 6: 34-37.
4. Diffie, W. 1982. Cryptographic Technology: Fifteen Year Forecast. Advances in Cryptography - A Report on Crypto81. Ed. Allen Gersho. Department of Electrical and Computer Engineering. Report ECE 82-04. University of California, Santa Barbara.

5. Diffie, W. and M. Hellman. 1977. Exhaustive Cryptanalysis of the NBS Data Encryption Standard. Computer. 10(6): 74-84.
6. Feistel, H. 1970. Cryptographic Coding for Data-Bank Privacy. IBM Research Report RC2827. Yorktown Heights, NY,
7. Feistel, H. 1974. Block Cipher Cryptographic System. U.S. Patent No. 3798359.
8. Feistel, H. 1974. Step Code Ciphering System. U.S. Patent No. 3798360.
9. Feistel, H. 1974. Centralized Verification System. U.S. Patent No. 3798605.
10. Grossman E. and B. Tuckerman. 1977. Analysis of a Feistel-Like Cipher Weakened by Having No Rotating Key. IBM Research Report RC6375. Yorktown Heights, NY.
11. Konheim, A. 1981. Cryptography, A Primer. New York: John Wiley and Sons.
12. Meyer, C. and S. Matyas. 1982. Cryptography - A New Dimension in Computer Data Security. New York: Wiley-Interscience.
13. National Bureau of Standards 1976. Data Encryption Standard. FIPS Publication 46. Gaithersburg, MD.
14. Paige L. and J. D. Swift. 1965. Elements of Linear Algebra. New York: Blaisdell Publishing Company.
15. Shannon, C. 1949. The Communications Theory of Secrecy Systems. Bell System Technical Journal. 28: 656-715.
16. Smith, J. L. 1971. The Design of Lucifer, A Cryptographic Device for Data Communications. IBM Research Report RC3326. Yorktown Heights, NY.
17. Smith, J. L. 1974. Recirculating Block Cipher Cryptographic System. U.S. Patent No. 3796830.

APPENDIX 1

```

00100      subroutine lucifer(d,k,m)
00200      implicit integer(a-z)
00300      dimension m(0:7,0:7,0:1),k(0:7,0:15),o(0:7)
00400
00500      c      message block stored one bit/location.
00600      c      key stored one bit/location.
00700      c      values must be 0 or 1. this subroutine doesn't verify that
00800      c      condition for message or key.
00900
01000      c      fortran stores data with innermost subscript varying the
01100      c      fastest, therefore, we have m(column,row,plane) and
01200      c      k(column,row), the rows are the bytes of the message and
01300      c      key, the columns are the bits in the bytes, for a normal
01400      c      language such as p1/1, we would declare m(row,column,plane)
01500      c      and k(row,column). we can equivalence a linear array of
01600      c      128 entries to the message and key because of the way
01700      c      in which they are stored.
01800
01900      dimension sw(0:7,0:7),pr(0:7),tr(0:7),c(0:1)
02000      dimension s0(0:15),s1(0:15)
02100      equivalence (c(0),h),(c(1),l)
02200
02300      c      diffusion pattern
02400      data o/7,6,2,1,5,0,3,4/
02500
02600      c      inverse of fixed permutation
02700      data pr/2,5,4,0,3,1,7,6/
02800
02900      c      S-box permutations
03000      data s0/12,13,7,10,14,13,11,0,2,6,3,1,9,4,5,8/
03100      data s1/7,2,14,9,3,11,0,4,12,13,1,10,6,15,8,5/
03200
03300      c      the halves of the message byte selected are used as input
03400      c      to s0 and s1 to produce 4 v bits each. if k(jj,ks)=0 then
03500      c      the low order 4 bits are used with s0 and the high order 4
03600      c      bits are used with s1, if k(jj,ks)=1 then the low order
03700      c      4 bits are used with s1 and the high order 4 bits are used
03800      c      with s0.
03900
04000      c      we don't physically swap the halves of the message or rotate
04100      c      the message halves or key. we use pointers into the arrays
04200      c      to tell which bytes are being operated on.
04300
04400      c      d=1 indicates decipher, encipher otherwise.
04500
04600      c      h0 and h1 point to the two halves of the message.
04700      c      value 0 is the lower half and value 1 is the upper
04800
04900      h0=0
05000      h1=1
05100
05200      kc=0
05300      if (d.eq.1) kc=8
05400
05500      do 100 ii=1,16,1

```

```

06400  c      c-i-d cycle
06500
06600      if (d,eq,1) kc=mod(kc+1,16)
06700
06800  c      ks is the index of the transform control byte
06900      ks=kc
07000
07100      do 200 jj=0,7,1
07200
07300          l=0
07400          h=0
07500
07600  c      construct the integer values of the hexdigits of one byte
07700  c      of the message.
07800  c      call compress(m(0,jj,h1),c,2) is equivalent and simpler
07900  c      but was slower. c(0)=h & c(1)=l by equivalence.
08000
08100      do 400 kk=0,3,1
08200          l=1*2+m(7-kk,jj,h1)
08300  400      continue
08400
08500      do 410 kk=4,7,1
08600          h=h*2+m(7-kk,jj,h1)
08700  410      continue
08800
08900  c      controlled interchange and s-box permutation.
09000
09100      v=(s0(l)+16*s1(h))*(1-k(jj,ks))+(s0(h)+16*s1(l))*k(jj,ks)
09200
09300  c      convert v back into bit array format.
09400  c      call expand(v,tr,2) is equivalent and simpler but
09500  c      was slower.
09600
09700      do 500 kk=0,7,1
09800          tr(kk)=mod(v,2)
09900          v=v/2
10000  500      continue
10100
10200  c      key-interruption and diffusion combined.
10300  c      the k+tr term is the permuted key interruption.
10400  c      mod(0(kk)+jj,8) is the diffusion row for column kk.
10500  c      row = byte & column = bit within byte.
10600      do 300 kk=0,7,1
10700          m(kk,mod(o(kk)+jj,8),h0)=mod(k(per(kk),kc)+tr(per(kk))+
10800      1      m(kk,mod(o(kk)+jj,8),h0),2)
10900  300      continue
11000
11100      if (jj.lt.7.or.d,eq,1) kc=mod(kc+1,16)
11200
11300  200      continue
11400
11500  c      swap values in h0 and h1 to swap halves of message.
11600      jjj=h0
11700      h0=h1
11800      h1=jjj
11900
12000  100      continue

```

```
13300  c      Physically swap upper and lower halves of the message after
13400  c      the last round. we wouldn't have needed to do this if we
13500  c      had been swappins all along.
13600
13700      do 700 JJ=0,7,1
13800          do 800 kk=0,7,1
13900              sw(kk,JJ)=m(kk,JJ,0)
14000              m(kk,JJ,0)=m(kk,JJ,1)
14100              m(kk,JJ,1)=sw(kk,JJ)
14200      800      continue
14300      700      continue
14400
14500      return
14600      end
```

APPENDIX 2

```

00100  c      main program that uses Luifer
00200      implicit integer (a-z)
00300      data handle/0/
00400      dimension k(0:7,0:15),m(0:7,0:7,0:1)
00500  c      message and key arrays are equivalenced to 128 element linear
00600  c      arrays.
00700      dimension key(0:127),message(0:127)
00800      equivalence (k(0,0),key(1)),(m(0,0,0),message(1))
00900  c      input byte arrays for reading key and message
01000  c      input is in hex digits. 128 bits = 32 hex digits = 16 bytes
01100      dimension kb(0:31),mb(0:31)
01200
01300      write(6,1003)
01400      read(5,1004) (kb(i),i=0,31)
01500
01600      write(6,1005)
01700      read(5,1006) (mb(i),i=0,31)
01800
01900      call expand(message,mb,32)
02000      call expand(key,kb,32)
02100
02200      write(6,1000) (key(i), i=0,127)
02300      write(6,1001) (message(i), i=0,127)
02400
02500      if (.not. lib$init_timer(handle)) goto 800
02600
02700      do 500 i=1,500,1
02800
02900  c      encipher
03000      d=0
03100      call lucifer(d,k,m)
03200
03300  c      decipher
03400      d=1
03500      call lucifer(d,k,m)
03600
03700  500      continue
03800      if(.not.lib$show_timer(handle)) goto 800
03900  800      continue
04000      write(6,1001) (message(i), i=0,127)
04100
04200      call compress(message,mb,32)
04300      call compress(key,kb,32)
04400      write(6,1003)
04500      write(6,1007) (kb(i),i=0,31)
04600      write(6,1005)
04700      write(6,1007) (mb(i),i=0,31)
04800
04900  1000      format(' key '/16(1x,i1))
05000  1001      format(' plain '/16(1x,i1))
05100  1002      format(' cipher '/16(1x,i1))
05200  1003      format(' key ')
05300  1004      format(32z1.1)
05400  1005      format(' plain ')
05500  1006      format(32z1.1)
05600  1007      format(1x,32z1.1)
05700      end

```

APPENDIX 3

```
key
0123456789ABCDEFFEDCBA9876543210
Plain
AAAAAAAAAAAAAAAAABBBBBBBBBBBBBBBBBB
key
0 0 0 0 0 0 0 1 0 0 1 0 0 0 1 1
0 1 0 0 0 1 0 1 0 1 1 0 0 1 1 1
1 0 0 0 1 0 0 1 1 0 1 0 1 0 1 1
1 1 0 0 1 1 0 1 1 1 1 0 1 1 1 1
1 1 1 1 1 1 1 0 1 1 0 1 1 1 0 0
1 0 1 1 1 0 1 0 1 0 0 1 1 0 0 0
0 1 1 1 0 1 1 0 0 1 0 1 0 1 0 0
0 0 1 1 0 0 1 0 0 0 0 1 0 0 0 0
Plain
1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0
1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0
1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0
1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0
1 0 1 1 1 0 1 1 1 0 1 1 1 0 1 1
1 0 1 1 1 0 1 1 1 0 1 1 1 0 1 1
1 0 1 1 1 0 1 1 1 0 1 1 1 0 1 1
1 0 1 1 1 0 1 1 1 0 1 1 1 0 1 1
ELAPSED: 00:01:47.51 CPU: 0:01:41.17 BUFIO: 0 DIRIO: 0 FAULTS: 0
Plain
1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0
1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0
1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0
1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0
1 0 1 1 1 0 1 1 1 0 1 1 1 0 1 1
1 0 1 1 1 0 1 1 1 0 1 1 1 0 1 1
1 0 1 1 1 0 1 1 1 0 1 1 1 0 1 1
1 0 1 1 1 0 1 1 1 0 1 1 1 0 1 1
key
0123456789ABCDEFFEDCBA9876543210
Plain
AAAAAAAAAAAAAAAAABBBBBBBBBBBBBBBBBB
```

APPENDIX 4

```

00100      subroutine expand(a,b,l)
00200          implicit integer (a-z)
00300          dimension a(0:*),b(0:*)
00400
00500      c      a is the array in bit array format.
00600      c      b is the array in byte format.
00700      c      l is the length of the array b in hexdigits.
00800      c      a must be 4*l long.
00900
01000          do 100 i=0,l-1,1
01100              v=b(i)
01200              do 200 j=0,3,1
01300                  a((3-j)+i*4)=mod(v,2)
01400                  v=v/2
01500      200      continue
01600      100      continue
01700
01800          return
01900      end

```

```

00100      subroutine compress(a,b,l)
00200          implicit integer(a-z)
00300          dimension a(0:*),b(0:*)
00400
00500      c      a is the array in bit array format.
00600      c      b is the array in byte format.
00700      c      l is the length of array b in hexdigits.
00800      c      a must be 4*l.
00900
01000          do 100 i=0,l-1,1
01100              v=0
01200              do 200 j=0,3,1
01300                  v=v*2+mod(a(j+i*4),2)
01400      200      continue
01500              b(i)=v
01600      100      continue
01700
01800          return
01900      end

```

SOLUTION TO "MALICE IN WONDERLAND" - PAGE 54

[Editor's note. Warning! Before you look at the rest of this page be sure to examine page 54 very carefully. And if you have read page 54 then be sure you have given yourself a fair chance before you read the solution below.]

The introduction to the message mentions the use of "proper reflection" and the puzzle itself says, "start your search with some careful reflection." If you need a further clue the subtitle of Alice in Wonderland is Through The Looking Glass. All of this suggests that you examine a mirror view of the material.

After some elements of distraction in the message there are eight instructions, e.g., "First take 2, 3, 4,..." which combined with the Eight opening lines supports the probability of a message being hidden in those lines.

Follow the directions, take the specified number of letters in each line, hold them up to a mirror and you have:

ME upon a ONCE there WAS,	TI
OOM! cried the FACE on THE OLD paroom	WAV
floor,	
-poop-a-goop SANG the GIRLS in the CHORUS,	poop
od MUST be let WHEN the WOLF's AT THE door!	olo
HER went climbing with ARMS AKIMBO;	NOT
HO can you SEE by the dawn's FRAGRANT	OH W
light?	
lical PROPHETS are prancing in LIMBO,	pip
TERS and elephants DANCE in the NIGHT!	TI

REVIEWS OF THINGS CRYPTOLOGIC

LOUIS KRUH AND GREG MELLEN

WHO'S AFRAID OF A CRYPTIC WOOLF?

Hawkes, E. and P. Manso. The Shadow of the Moth: A Novel of Espionage with Virginia Woolf. St. Martin's/Marek, 175 5th Ave., New York, NY 10010, 1983, 280 pp., \$12.95.

A literate work of fiction has the famous writer, Virginia Woolf, involved in a murder mystery with spies and traitors in London, during WW I. The authors have cleverly placed Woolf and a number of her Bloomsbury friends alongside fictional characters to give the book a touch of realism. The plot is an exciting one, and book codes solved by the heroine play a prominent role. [LK]

WELL, PUZZLE THAT, WILL YOU?

Decipher, Inc. Pente Games, Inc., Box 1546, Stillwater, OK 74076, 1983, \$12.

This unusual game is a jigsaw puzzle which reveals a number cipher when assembled. Each number represents a single letter in the cryptogram and the company is offering \$100,000 as a cash award to the first person who solves it.

The inventor of Decipher got his idea from reading an article about the Beale cipher. As a result, a similar enciphering technique, i.e., use of a book, document or other easily available text for the key, has been used. The brochure accompanying the game calls it a multiple substitution cipher and explains that each letter in the alphabet can be represented by many different numbers. Clues are provided, including, "The key is in the public domain — you have easy access to it." Authenticity of the cipher and the \$100,000 prize is guaranteed by an insurance company, and the solution is locked in a vault of a major bank in New York City. So, although solving the Beale cipher may bring a larger reward, with this cipher you have the assurance that it is genuine. Decipher is available in stationery departments and where adult games are sold. [LK]

WORD PUZZLE PROGRAMS

Mau, E. E. Create Word Puzzles With Your Microcomputer. Hayden Book Co., 50 Essex St., Rochelle Park, NJ 07622, 1982, 304 pp., \$14.95.

This book contains a collection of 17 computer programs which produce 25 puzzles including simple substitution cryptograms, acrostics, word-finds, letter shuffle and other word puzzles. The programs provide either blank puzzles with answer keys or printouts following puzzle magazine format. Each puzzle type and data base is illustrated in detail showing the type of print-out that can be achieved. Complete information is provided on establishing and maintaining the necessary word and quotation files that form the data bases. The book, therefore, also serves as a general tutorial on non-numeric data handling. All programs are written in Microsoft's BASIC-80 and may require varying degrees of program modification for some computers and special attention is given to these conversions. [LK]

SINKOV GAINS WEIGHT

Elementary Cryptanalysis: A Mathematical Approach, Abraham Sinkov, The Mathematical Association of America, 1529 18th St. NW, Washington DC 20036: New Mathematical Library No. 22, 3rd printing, 1980, \$8.75, paper.

There is nothing on the cover or spine to suggest that this third printing of what has become a cryptologic staple differs from previous printings. It is in fact a second edition, meeting the dictionary criterion "a printed production the same as an earlier one but with substantial...additions."

Professor Paul L. Irwin of Randolph Macon Women's College has contributed a supplement of five BASIC programs: Index of coincidence; matching alphabets; digraphic frequency distribution; trigraphic frequency distribution (mono-alphabetic), and trigraphic frequency distribution (polyalphabetic). Intended for use in a course in cryptanalysis at Virginia's Governor's School for the Gifted, the programs give the student the opportunity to test techniques described by Dr. Sinkov using cryptograms of the student's choice.

Programs are listed twice, once in DECSYSTEM-20 dialect and again for the H-P family. The former are heavily interactive for student participation and are well documented by REMs. Most computer users will want to adapt the second versions for their own use — not a difficult task.

I am indebted to Professor Irwin for calling this reissue to my attention, else I would probably remain ignorant of it, already having the first edition.

The programs include Trigraphic Frequency Distribution, Index of Coincidence, Matching Alphabets, and Digraphic Frequency Distribution. The book, one of the best on the subject, introduces the reader to the mathematical aspects of cryptanalysis. It starts out with monoalphabetic ciphers and proceeds through polyalphabetic substitutions, polygraphic systems and transposition ciphers. Mathematical topics touched include modular arithmetic, number theory, some linear algebra of two dimensions with matrices, a bit of combinatorics and some statistics. These subjects are integrated with the cryptanalytic techniques explained by the author. The book is very suitable for use as a textbook with exercises at the end of each chapter and the solutions at the end of the text. Sinkov, who was hired by W. F. Friedman in 1930 and worked as a cryptologist for the War Department and the Department of Defense for over 30 years, has done a fine job in making a complicated subject comprehensible. [LK, GM]

THE COMPUTERS ARE COMING!

Burnham, D. The Rise of The Computer State, Random House, 201 E. 50 St., New York, NY 10022, 1983, 273 pp., \$17.95.

In a disturbing examination of America's computerization, the author shows how much information credit agencies, IRS, FBI, Social Security, government intelligence agencies, telephone companies, cable and other firms know about each of us. Just as important, if not more so, how more and more of that information is being put to unexpected and sometimes, even sinister, use. The book not only discusses data bases, two-way cable systems, electronic funds transfers and computerized communication systems but also how organizations use these systems and how these systems influence the way we think and reveal our behaviour patterns. With one exception, the activities of the computer dominated organizations are covered in chapters devoted to broad topics. The exception is the National Security Agency, which is said to have "a massive bank of what are believed to be the largest and most advanced computers now available to any bureaucracy on earth." This chapter, which relates some fascinating incidents, is subtitled, "The Ultimate Computer Bureaucracy." [LK]

PUBLIC KEY TEXT

Merkle, R. C. Secrecy, Authentication, and Public Key Systems. UMI Research Press, 300 N. Zeeb Rd., Ann Arbor, MI 48106, 1982, 104 pp., \$34.95.

A revision of the author's 1979 PhD thesis at Stanford University, which concludes, "that many of the techniques described in this study will be used

in telecommunication systems that span the globe to protect the privacy and integrity of communications of all kinds." This mathematically oriented report includes the following chapters: One Way Hash Functions, A Public Key Cryptosystem Using Puzzles, Public Key Distribution Using Puzzles, A Certified Digital Signature, The Trapdoor Knapsack, How Secure is The Trapdoor Knapsack, An NP-Complete Conventional Cipher, Protocols for Public Key Cryptosystems, and On the Security of Multiple Encryption. Considering the complexity of the subject, Merkle manages to provide a generally clear and succinct presentation of these recent cryptographic concepts. [LK]

INTRODUCTION TO CRYPTOLOGY - AUF DEUTSCH

Franke, H. W. Die Geheime Nachricht. Umschau Verlag, Sigma Studio Presse, Stuttgarter Strasse 18-24, 6000 Frankfurt am Main 1, West Germany, 1982, 208 pp., \$14.

The publisher claims this is the first comprehensive work in German which provides a general introduction to cryptology. The first half of the book is a history of cryptology from the skytale to the Enigma. It reviews the work of pioneers such as Trithemius, Porta, Vigenere, Kasiski, Friedman, and others. The second half of the book deals with electronic developments, data security, voice scrambling, and public-key cryptography. It is an attractive book with many illustrations and excellent photographs of cipher devices. Also included is a separate sheet of cardboard imprinted with the two sections of a cipher disk to cut out and assemble. [LK]

COLOSSUS FEATURED IN HISTORY OF COMPUTER JOURNAL

Colossus at Bletchley Park, a special feature including The Design of Colossus, T. H. Flowers; The Making of Colossus, A. W. M. Coombs; The Installation and Maintenance of Colossus, W. W. Chandler; plus a Foreword by H. Campaigne. Annals of the History of Computing, July 1983, pp. 239-262. c/o AFIPS Press, 1815 N. Lynn St., Arlington, VA 22209. Back issues of the magazine, \$12 for nonmembers of AFIPS, \$9 for members.

During WW II, the Germans used machine-enciphered teleprinter messages for upper echelon communications. The cipher machine, called "Geheimschreiber" by the Germans and "Fish" by Allied cryptanalysts, was much more complicated than the Enigma and its messages were usually more important. The Colossus, which was, in essence, an early digital, electronic, programmable computer, was designed to help decrypt the Geheimschreiber ciphers. Flower's article

describes the construction and operation of the Colossus machines; Coombs relates the techniques that evolved for their design and manufacture; Chandler describes the procedures adopted for the installation and maintenance of the Colossus machines at Bletchley Park; and Campaigne's brief Foreword puts the articles into perspective from his view as a cryptanalyst-programmer using the Colossus. [LK]

CRYPTOLOGIC MUSEUM

Though we're seven years late and this reviewer has not seen it, Cryptologia takes note that the Rear Admiral Joseph Numa Wenger Naval Cryptologic Museum has been established at Headquarters, Naval Security Group Command, 3801 Nebraska Ave. NW, Washington, DC 20390. Described as "tiny," the museum honors the late RADM Wenger, who served in naval cryptography (the first flag officer to bear the cryptologic specialty designator) for 46 years.

The announcement we have states, "The museum is open to retired NAVSECGRU personnel and their families by appointment,"; that doesn't say it's closed to everyone else. The Historian/Curator may be reached at the address above (Attn. G-10), or at (202) 282-0873. [GM]

THE STORY OF THE ON-THE-ROOF GANG

Intercept Station "C": From Olongapo through the Evacuation of Corregidor, 1929-1942, Sidney A. Burton et al., Naval Cryptologic Veterans Association, 3065 Olive St., Denver, CO 80207, 1983, 83 pp., \$9.

Largely a collection of first-person "sea stories" by the eight main authors, this volume is heavier on human interest than on the cryptologic achievements of the Naval intercept station in the Philippine Islands. However, that is what it was intended to be, and it meets its purpose admirably. The history of how the station was established, manned and equipped and of how it evolved before and during World War II is well worth the purchase price, though the reader who wasn't there may find the myriad names a bit confusing at times — keeping in mind that "myriad" is from the Greek for "ten thousand." The volume is profusely illustrated with personal photographs taken by the authors. [GM]

ONE A DAY

Ladd, C. D. 365 Cryptograms. Cryptos, Box 7705, St. Paul, MN 55119, 1983, 72 pp., \$ 6.95 ppd.

A collection of 365 cryptograms, one for each day of the year. The messages are clever sayings and often humorous. Introductory comments provide tips for solving. Large easy-to-read type is used for the cryptograms with answers in much smaller size at the back of the book. Excellent gift for youngsters or oldsters. [LK]

NORSE KILROY WAS HERE

Syversen, E. Norse Runic Inscriptions, With Their Long-Forgotten Cryptography. Vine Hill Press, 5855 Vine Hill Rd., Sebastopol, CA 95472, 1979, 123 pp. \$8.95.

The late Alf Monge, a WW II cryptanalyst, spent a great deal of time trying to prove that ancient runic inscriptions contained secret messages and dates. The author, a close friend of Monge, who also did cryptographic research on runic inscriptions, details the cryptography and methods by which the solutions were discovered. The book deals with rock carvings found in Scandinavia, Greenland, Orkney and Shetland Islands, and North America. Whether or not you agree with the conclusions, it is an interesting work profusely illustrated with many photographs of rune stones inscriptions and detailed charts of the cryptanalytic techniques involved. [LK]

ENIGMA AND GENERAL CRYPTOLOGY MATERIAL

Rollema, D. W. Enigma, A Detailed Examination of the German World War II Cipher Machine and the Cracking of the Code. Wireless World, Quadrant House, The Quadrant, Sutton, Surrey SM2 5AS, England, June 1983, pp. 49-54. Back issues \$2.60 each.

Excellent article with many photographs detailing the workings of the Enigma and how Polish cryptanalysts solved its enciphered message.

Hawker, P. Electronic Cryptography. Codes, Ciphers, Communications and Computers. Wireless World (address AND COST above), September 1980, pp. 44-49.

An encyclopedia-like article covering some basics of cryptography, digital coding, security of cods, data encryption standard, public-key systems and cryptanalysis. [LK]

KEEPING ABREAST WITH CURRENT ELECTRONICS

Military Electronics. 1980. The International Defense Review Special Series - 9. Interavia USA, 1741 N. Ivar St., Los Angeles, CA 90028. 212 pp. \$17.00

International Defense Review (IDR) is a large-size, 9" X 12", high quality, \$75 per year magazine published in Switzerland, which is devoted to defense systems of every type such as armaments, aircraft, vessels, communications, and all other material used by nations for their defense or to conduct an all-out war. The Special Series consists of 12 titles at present, each containing a collection of articles on a particular subject, which have appeared in (IDR) since 1976.

The Military Electronics volume includes sections on Command, Control and Communications (C³), military computers, Radar and AEW, Monitoring Systems, Laser Systems, and Trends in Technology.

The C³ section contains an excellent 3-part, profusely illustrated set of articles on cryptology by Kirk Kirchhofer, now with Crypto AG, plus his separate article on Secure Voice Communication. These articles cover the subject in a knowledgeable and authoritative fashion.

Other articles discuss secure battlefield communications, base security, and electronic intelligence gathering. There are also reports on defense exhibitions which provide a brief insight into recent products and systems including communications security equipment. [LK]

BEALE CYPHER SOCIETY NEWS

Proceedings of the Third Beale Cipher Symposium 1981. Beale Cypher Assoc., Box 216, Medfield, MA 02052. 107 pp. \$15.00.

The ten presentations included in the Proceedings contain a great deal of information on the Beale cipher including several analyses of its contents with various frequency counts, techniques for solving the cipher, an analysis by this writer suggesting that the whole thing is a hoax, and one solution. Two especially worthwhile articles are "High Order Homophonic Ciphers" by Dr. Carl Hammer and "The Book Cipher by Nicholas Trist" by Dr. Albert C. Leighton and Dr. Stephen Matyas. Both newcomers and longtime aficionados of the Beale cipher will find the 1981 Proceedings most informative. [LK]

CRYPTO-PROJECT

For the past few years, Dr. and Mrs. Richard V. Andree, with the support of the National Science Foundation, the University of Oklahoma and the National High School and Junior College Mathematics Club (Mu Alpha Theta), have been developing material for teaching mathematics and logical thinking. Five mini-courses are available and four of them involve cryptology.

The materials are mainly for secondary students but they have been used successfully with elementary students and adults in various test sites from New York to California. Following are descriptions and prices for each of the units.

Secret Ciphers. This cartoon presentation of techniques for solving simple substitution ciphers is designed to interest students who are indifferent to ordinary mathematics. It won't make great mathematicians of them, but will start them using logic and common sense to decipher secret messages. Single copies: \$3.50 plus \$0.75 handling. Includes instructor's manual. Classroom quantities may be purchased for \$2.00 in sets of ten or more.

Solving Ciphers. A more advanced presentation, still in casual cartoon style, teaches breaking substitution ciphers both with and without word divisions, using frequency distributions and pattern words. A suitable sequel to Secret Ciphers, or maybe used as a first introduction for more mature students. Prices are same as for Secret Ciphers above.

Sophisticated Ciphers. This volume assumes some understanding of simple substitution ciphers, as would be gained from either of the above volumes. It presents advanced cipher methods including Playfair, Hill Matrix, and modern encipherment machines. The Hagelin cryptographer and the Japanese "Purple" machine are discussed. This fascinating presentation shows unexpected applications of modern mathematical methods to the science of cryptology. It is more advanced than the other two cipher volumes, but still easily understood. Prices are the same as for Secret Ciphers above.

Cryptarithms. You can start with this at any level. It is just about the most carefully written elementary material available on cryptarithms--those tantalizing little puzzles made by substituting letters for digits in an arithmetic statement, like $SEND + MORE = MONEY$. Over 200 cryptarithms along with careful descriptions of the logic used in solving them, and for creating one's own cryptarithms; carefully prepared material on generalizing the techniques used and transferring them to the solution of real life problems unrelated to mathematics. Single copies: \$4.50 plus \$0.75 handling. Includes instructor's manual. Classroom quantities may be purchased for \$2.90 each.

Logic Unlocks Puzzles. Presented for the average and better high school student interested in solving problems--not just problems in algebra and geometry, but real life social problems as well. The currently developing science of "how experts use common sense to attack problems" is presented in understandable terms without the usual jargon and technical terms. Price is same as for Cryptarithms above.

For \$20 plus \$1.56 postage (and \$2 billing fee if not prepaid) you can get all five booklets with the five instructor's manuals and supplementary instructional materials. CRYPTO-PROJECT, 601 Elm, RM 423, Norman, OK 73019. [LK]

OLD TECHNIQUES GET NEW LIFE

Whenever there may be a real or perceived need, regardless of what kind it is, you can be sure that, just as nature abhors a vacuum, some enterprising firm will spring up to fill the void.

In the shadowy world of mercenaries, soldiers of fortune and private security forces there undoubtedly is a need for secure communication. For various reasons, including an economic one, this need falls short of a requirement for sophisticated and costly cryptographic equipment. In addition, there may be businesses whose demands for communications security are also of a lower level than that supplied by the relatively expensive cipher machines on the market.

To fill this gap, a small firm, TAC COM, Box 3255, York PA 17402 has developed a line of traditional pencil and paper ciphers. It includes 40-page Random Number Pads, 2.5" x 3", with instructions, for \$100. per set of two. There is a Cipher Matrix, 5.5" square for \$7., which is actually a Vigenere cipher consisting of the regular alphabet plus the ten digits to provide for alphanumeric encipherment, and to make it rugged and waterproof for field use it is encased in 10 mill laminated plastic with instructions on the back. Another version for \$10, termed a Commando ParaCipher, features a random arrangement of the numbers and alphabets. Also available for \$25. is a 37 page booklet with 26 Authentication Tables/Cipher Squares and instructions for preparing digraph ciphers. A folder describing the complete line is available on request. [LK]

SCI FI NUMERICAL CODE

Asimov, Isaac and A. Laurance, eds. 1982. Speculations. Boston: Houghton Mifflin Co. 288 pp. \$12.95.

Science fiction lovers will get special enjoyment from this collection of 17 short stories by well-known science fiction authors whose names are given in

code at the beginning of each story. Experienced science fiction readers are supposed to recognize the writers from their style of writing and everyone can refer to the instructions in the back of the book, which gives the key to a simple sub numerical code. [LK]

A MODERN CRYPTOLOGY TUTORIAL

Davies, D. W. Tutorial: The Security of Data in Networks. IEEE Computer Society Press, Box 80452, Worldway Postal Center, Los Angeles CA 90080. 1981. 241 pp. \$20.00 for non-members, \$15.00 for members.

The purpose of this tutorial is to present the major advances that have occurred since 1976 in the application of cryptography. It is organized in two sections. Part I is devoted to the Data Encryption Standard and Part II is concerned with public key cryptosystems and their applications. The author introduces each section with an excellent outline of the concepts involved and he has made a wise selection of papers to cover the two main topics. The 22 reprinted papers include, "Privacy and Authentication: An Introduction to Cryptography" by Diffie and Hellman; "New Directions in Cryptography" by the same authors; "Some Cryptographic Techniques for Machine-to-Machine Communications" by Feistel, Notz and Smith; "Secure Communications Over Insecure Channels" by Merkle; papers by Rivest, Shamir and Adleman, plus many other important articles published in the past few years. Davies also provides an annotated bibliography. [LK]

INTELLIGENCE BIOBLIOGRAPHY

Constantinides, G.C. Intelligence and Espionage: An Analytical Bibliography. Westview Press, 5500 Central Ave., Boulder, CO 80301, 1983, 559 pp., \$60.

The author, who has spent almost 25 years in U.S. government intelligence and national security work, has justifiably described his book as "the most comprehensive and thorough bibliography of English-language nonfiction books on intelligence and espionage to date." It is an enormous work with knowledgeable comments, most of them a page or more, on close to 500 books. In a special category index the author has divided them into 54 categories. The bibliography itself is arranged by author. One of the categories is Communications Intelligence, Cryptology, and Signals Intelligence which contains 40 books. Constantinides demonstrates a familiarity and expertise in the subject matter with incisive comments and cross references in many of his annotations.

In his remarks on Yardley's American Black Chamber, he provides views from five other authors and suggests areas in Yardley's career which still need to be explained. With Lewin's Ultra Goes to War, he refers to reviewers of the book as well as other authors to point out inaccuracies and to remind us that because much Ultra material is still secret, the full story has not yet been told. In his overall excellent appraisal of The Codebreakers, he expresses possibly an insider's view that Kahn's assessment of Friedman as being responsible for the U.S.' cryptologic superiority is questionable. Other worthwhile comments abound in this outstanding reference work which will be consulted frequently by persons seeking a guide to intelligence literature. [LK]

YARDLEY'S CHINESE CONNECTION

Yardley, H.O. The Chinese Black Chamber; An Adventure in Espionage. Houghton Mifflin, 52 Vanderbilt Ave., New York, NY 10017, 1983, 225 pp., \$13.95

In 1938, Chiang Kai-shek, head of the Nationalist Chinese government which was fighting a desperate losing battle against the Japanese, engaged Yardley to come to the war torn capital of Chungking to set up a Chinese version of the American Black Chamber. Yardley had organized and directed in New York. This manuscript, hidden for over 40 years, is the story of his adventures and intelligence exploits in China from 1938-1940. Most of the account is a fascinating glimpse of life in a strange society of Chinese characters, European traders, politicians, generals, spies, traitors, mistresses and other colorful personalities. Few of Yardley's cryptanalytical episodes are included but he does describe, step-by-step, how he solved a cipher which used a public Chinese code book superenciphered by a book cipher. The book has an introduction by James Bamford, author of The Puzzle Palace, with additional details of Yardley's experiences in China. It concludes with "Memories of the American Black Chamber", a brief memoir by the author's wife, Edna Yardley, who is its last surviving original member. [LK]

POCKET BOOK CRYPTOGRAMS

Ciphers. Raja Books, Box 2365, Norman OK 73070. 1983. 38 pp. \$1.00 plus \$0.35 postage or \$10.00 for a dozen assorted titles.

A pocket size book with simple substitution ciphers, tips on how to solve, and answers are given in the back of the book. Other titles in the series include Cryptarithms, Puzzle Potpourri, Math Puzzles, Small Crossword Puzzles, and Word Puzzles. [LK]

WHO DID IT?

LOUIS KRUH

The following item, reprinted in its entirety, was found in the files of a long time member of the American Cryptogram Association.

It is not always the butler who did it. In a recently published detective story, the detective upon proper reflection discovered in the following message a concealment cipher that told him who did it. Can you discover the same message?

MALICE IN WONDERLAND

TIME upon a ONCE there WAS,
ZAWOOM! cried the FACE on THE OLD baroom
floor,
boop-boop-a-doop SANG the GIRLS in the CHORUS,
blood MUST be let WHEN the WOLF's AT THE door!
MOTHER went glimbling the ARMS AKIMBO;
OH WHO can you SEE by the dawn's FRABJOUS
light?
biblical PROPHETS are prancing in LIMBO,
TIGERS and elephants DANCE in the NIGHT!
Now if you'd perform a fine feat of detection
You'd best start your search with some careful
reflection:
First take 2, 3, 4, 3 and then 3, 3, 3, 2,
And the name of the killer will peer back at you.

Although this mystery message is more steganographic than cryptographic, readers might enjoy the challenge of finding the solution.

If you can't figure it out, look around this issue.

CRYPTANALYSTS' CORNER

GREG MELLEN

The cover of this issue shows an implementation of the Wheatstone cipher disk. The device is of unknown provenance but the engraved plaintext and printed ciphertext alphabets are Danish.

The device is 3.0 inches in diameter and weighs 12.5 ounces. The rear is a solid metal plate engraved with a crown, under which is "7 IK" with a "2" below that.

Both covers may be unscrewed. The rear cover gives access to a circular storage space for about a dozen thin cardboard ct disks. The floor of the storage area is a screwed solid plate protecting the gears.

Several of the ct disks have pencilled Danish mixed alphabets, and the remainder are blank. By taking off the front cover, the ct disk may be replaced.

The history of the Wheatstone cipher disk is described by Kahn [1] and its cryptanalysis by Friedman [2]. Friedman's treatise is quite complete, covering an important variation of the system in which the pt alphabet is also mixed. Unlike several machine ciphers, the Wheatstone disk system and its variants are trivial to program. The shorter alphabet simply slides against the longer one after each complete revolution of the disk.

With regard to the device on the cover, the deviations from Wheatstone's original system are three in number, all trivial:

1. The ct alphabet is 29 characters long and the pt 30, to accommodate the Danish alphabet, plus the "Q" and the space. (The "Q" is red—the other characters are black—and is apparently the mark against which the ct alphabet is set at the beginning of each message.)
2. Turning the stem turns both ct and pt alphabets. The arrow is clearly the direction of choice, but the stem rotates the alphabets in either direction, and the ct alphabet slides one step per full revolution. Pressing the button beneath the stem holds the ct disk fast, permitting the initial setting of the ct-pt alignment.

3. The ct is the outer rather than the inner alphabet.

The unit has a heavy leather protective cover embossed with the same "7 IK" over "2" as noted above. The crown is stamped as with a roller on the inside of the case. A buckled strap, which is too flimsy to serve as a carrying loop, holds the cover closed.

All in all I judge the device to date from the time of World War I. It obviously has received heavy, but by no means abusive, use. Local inquiries have not yielded any further information. I would appreciate hearing from any reader who believes he can shed further light on the history of this unit.

We have about concluded, at least for a time, the topics discussed for the past year or so: isomorphs, alphabet reconstruction, progressive systems and so on. I would like to begin what Kahn once referred to, in a place I no longer remember but in a phrase which I recall because of its uncharacteristic inaccuracy, as "deadly dull exercises in symmetry of position." Those who may want to review patent symmetry may want to see reference [1, p. 237-8].

Symmetry of position is useful in situations where the same cipher components are used in several relative positions. Vigenere is a trivial example: Once a single ct-pt correspondence is identified, the remaining correspondences are immediately known. (There is no "true" decimation; they are all equally valid. For the standard alphabet, the A, B, C... sequence is no more true than any other, it is simply better known. It is always valuable though to recover the one originally used by the encryptor in order to determine the keyword, and thus, gain further insight into his thought habits.)

Interestingly, though I can't think why anyone would want to do it, a similar situation holds true even if several different decimations of the standard alphabet are used as cipher components. Once two ct-pt correspondences in the same component are known, the decimation may be identified and the entire component recovered. This is a fortunate property since, owing to the malevolence of nature, the original decimation is seldom recovered by symmetry of position.

Usually, this column concludes with an explanation of the cipher system and the messages in the previous column. This time will be an exception for the benefit of those readers who have not solved last issue's messages as yet, but may lately have achieved an intuition. For those readers who had solved the prior messages, I will add a few messages in basically the same system, perhaps with a simple change to make them somewhat harder.

1. FFQO 2RUCN UMXUE QWXTZ HUI3Y IX02L MKCT3 DARVS THIEZ KEFMP GNYWF
QRRBE WDLZX FRYPM JV2P3 UVMWR Q2CEV 32V4Z LXAPN BASDR 2FTAR JGOSE
C3RNF VRLBP 2M2FH RGBAU ANRVM BA2DS HHDY3 XFJZC GEIT4 YHWUO FKELX
VEW4G IIIZE WBQXC HRQHS UNSXX
2. 33GAC VCZQS NKXN3 3HVUB PMKEM QQNTP CVBJJ QYVU2 SBIVK YHLAJ SZTT3
QMWTs RICH0 TTD0M H3HIY HD3XM OZQIC BLKTB JJOZZ KXJVJ OZESZ BE24F
3DKSV HTSCI SDUN3 OGFQS KZGCE QXCHR QHRML ZYPKZ AC RTP 4PI2J AJSKQ
ZKK3J KDF4W TKWXX
3. MMYJ4 UXF2S HH43P TXLCC P4J3T FRAS T XAMLF XFETH NHYDZ LQE3M GX4UV
NC4ME AJZW4 VL4ZL YGAEP KPTS4 ECUWB CHEOF BHITN D3JLD MLWFN QNCTH
UV2IO NNPWK Q42AD U2XNJ AOXJE BZFET QTOAF PEILF B3FB3
4. BSDFL BMVUG LKQ40 OURZ3 LSXXZ UVR3K FW43L WBSKL KC30D OMANS ECRBP
LUGHD XUBCW VNIUH SUNSM PWCZY Z34UC XGLJX OC2KJ OT3DA RVSAB SIKDE
DX3OG HQT2D DZIYE UQWAG QLDVW 2LVCJ NKC3E 32WKZ CTSKZ RKJR4 NCMB5
YZMDO MB24I BRFJC NMX4N 3HYMO SWM2Y SC3UC XGHJ4 KXXXX

REFERENCES

1. Kahn, D. 1967. The Codebreakers. New York: The Macmillan Company. pp. 197-8.
2. Friedman, W. F. 1918. Several Machine Ciphers and Methods for their Solution. Publication No. 20, Riverbank Laboratories. pp. 6-36. [Reprinted: Laguna Hills, CA: The Aegean Park Press. Vol. 2 in the Riverbank Publication Series. 1979.]

LETTERS

Dear Editor,

This letter is written concerning the article, "Applications of Vincent's Theorem in Cryptography," by Alkiviadis G. Akritas which appeared in Cryptologia, Volume 6 Number 4 (October 1982), pp. 312-318. You do students of cryptography a considerable disservice by publishing this article. I am amazed that it survived the editing process and, further, that it survived a referee.

A "one time pad" is unconditionally secure only because the information required to reconstruct the key is as great as that required to transmit the message. Any key that may be transmitted by a lesser amount of information does not preserve the quality of unconditional security. There should be no doubt of this fact.

Even though the technique presented by Akritas may be useful it is definitely not a one time pad. A one time pad requires that each key element be independent and identically distributed. Key elements that are created by Akritas' method are not independent, even if they happen to pass commonly used statistical tests.

Ron Crandall, 3859 Gleason Ave., San Jose CA 95130

Author's response:

In response to Mr. Crandall's remarks we have to admit that a better title for our paper would have been, "Applications of Vincent's Theorem in Cryptography or a proposal for the perfect one-time pad scheme" (instead of "Applications of Vincent's Theorem in Cryptography".) However, despite the title, we definitely state in our paper that we do not have a problem-free one-time pad scheme and we, ourselves, point out the various "things to watch for and topics for further research" (p.316.) Given the fact that the purpose of our paper was to "stimulate the reader for further research on the subject" we are sorry to see that it caused Mr. Crandall so much frustration, agony and despair.

Alkiviadis G. Akritas, Department of Computer Science, The University of Kansas, Lawrence KS 66045

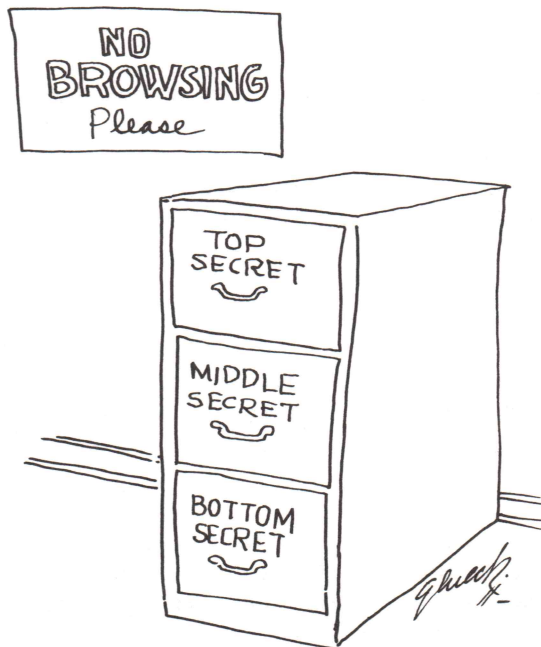
Editor's response:

Mr. Crandall is totally correct when he says that "a 'one-time pad' is unconditionally secure..." Professor Akritas, in his article is also totally correct and agrees with Mr. Crandall, as his opening sentence indicates: "...one-time pads are unconditionally crypto secure."

Perhaps Mr. Crandall's objection arises because he interprets Professor Akritas' technique as being identical to a one-time pad and therefore as theoretically secure. The sub-title of the article, "One-time Pads Made More Practical," in my opinion alerts the reader that the author does not imply identity and the reader should not infer it.

I may have been one of the referees — I do not recall. If so, I plead guilty to a misdemeanor but not to a felony. I should have suggested changing the first sentence of the second paragraph of the article to: "In what follows, we propose a pseudo-one-time pad scheme..." The prefix would have emphasized the implication of the subtitle.

Greg Mellen



CIPHER MACHINE INVENTOR - BORIS HAGELIN DIES

DAVID KAHN

Boris C. W. Hagelin, the world's most successful inventor of cipher machines, died September 7 1983 in Zug, Switzerland, aged 91.

Hagelin was the first and probably the only person to become a millionaire from cryptology. He did it through the creation and sale of a compact cipher machine. More than 140,000 were manufactured during World War II for the U.S. Army, which called it the M-209.

A tallish, white-haired, kindly man, Hagelin had a gentle humor about him. He was once asked whether he spoke five languages fluently. "Only one at a time," he said with a smile. In his pockets he carried peanuts to feed birds. But despite his lack of pretension he lived well, driving expensive cars and dining on perfect souffles made by his cook. He owned homes in Zug and in his native Sweden.

Hagelin, a mechanical engineer, was put into a Stockholm cipher machine firm in 1922 to watch over the interests of his father, who had invested in it. When the founder died, the Hagelins took over, Boris improved some mechanisms and sold them, but his first break came when the French general staff asked him in 1934 to devise a pocket-sized cipher machine that would print its output and so permit one-man operation.

He whittled a piece of wood that would fit into a pocket to show the machine's size. Then, one day he thought of a small cylindrical cage with lugs that he had constructed as a number-adding device for a vending machine. He combined it with other elements to create an intricate but rugged mechanism that has been called "a jewel" and that generated a cipher of fair complexity.

The French bought it and, in a later version, the M-209, so did the Americans. The U.S. Army used it for secret communications from battalion level to division. Though the Germans occasionally solved cryptograms enciphered in it, these solutions came too late for operational use.

The machine's success attracted business to Hagelin after World War II, as former colonies became independent nations needing secure communications for their soldiers and their diplomats. In 1959, he moved his company to Switzerland, where the laws made it easier and more profitable for him to operate. Crypto AG (Aktiengesellschaft, or Incorporated) prospered first in Zug, then in nearby Steinhausen.

As its products became increasingly electronic, and as he grew older, Hagelin took less and less of an active role in the firm, though he retained his interest in it and in cryptology. He eventually sold Crypto to the German electrical giant, Siemens, as a subsidiary, of whose board he remained honorary president.

FROM THE ARCHIVES
THE ACHIEVEMENTS OF THE CIPHER BUREAU (MI-8)
DURING THE FIRST WORLD WAR
DOCUMENTS BY MAJOR HERBERT O. YARDLEY
PREPARED UNDER THE DIRECTION OF THE
CHIEF SIGNAL OFFICER
25 MAY 1945
SPSIS - 1
SIGNAL SECURITY AGENCY, WASHINGTON, D.C.

(Declassified per Sec. 3, E. O. 12065 by Director, NSA/Chief, CSS, 11 April 1979.)

[Ed. Note. During the course of their research, our editors and readers are sometimes responsible for the declassification of previously undisclosed material. Or they may discover items in private or public collections, libraries, and archives, items which are not widely known. The purpose of this column is to give these documents wider circulation for the benefit of the cryptologic community. If you have or know about material suitable for this column, please send it to David Kahn, 120 Wooleys Lane, Great Neck, NY 11566. All contributions used will credit the donor.]

[Louis Kruh ran across a reference to this column's document and requested a declassification review. As a result, it was declassified on 11 April 1979.]

[The text with the original Editor's Foreword follows.]

This paper presents verbatim transcripts of a number of historical documents now in the files of the Signal Security Agency. They describe the achievements of the Cipher Bureau (MI-8) maintained by the Military Intelligence Division in Washington from 1917 to 1919, and its successor, the cryptanalytic unit directed in New York City by Mr. Herbert O. Yardley. Though the latter unit continued to exist until 1929, the data here presented are for the most part no later than 1920.

While these documents provide much material of historic interest, they are in no sense regarded as adequate accounts of the work of these units, but are now published primarily to afford an opportunity for comparison with the statements made by Mr. Yardley in The American Black Chamber (1931). Only one of the documents is signed but there can be no doubt that they are all the work of Mr. Yardley.

Footnotes which are unsigned are by the editor. Those marked "W.F.F." are by Mr. William F. Friedman; those marked "H.O.Y." present the contents of remarks on slips of paper inserted by Mr. Yardley.

11 May 1945

CONTENTS

A history of the Code and Cipher Section during the First World War, prepared in 1919 by Major Herbert O. Yardley.

M.I 8 [1]

Code and Cipher Section [2]

Origins.

When war was declared, neither the War Department nor any other department of the Government possessed even a rudimentary organization for attack on codes and ciphers. Colonel Van Deman [3] (then Major Van Deman) recognized, however, that such an organization was absolutely indispensable and immediately began a search for experts to form it and train the necessary personnel.

The only officers of the Army known as expert in the subject were Colonels Parker Hitt (then a Captain) and Joseph O. Mauborgne and Frank Moorman (then Lieutenants) [4]. Colonel Van Deman endeavored to procure the services of these officers but Colonels Hitt [5] and Moorman [6] were sent to France with the American Expeditionary Forces and Colonel Mauborgne [7] was assigned to

important administrative duties in the radio service of the Signal Corps. Accordingly it became necessary to find experts in civil life and enlist their services.

On June 10, 1917, a beginning was made by the commissioning as First Lieutenant (later as Major) of Herbert O. Yardley, who had several years' experience in code work in the State Department and had incidentally developed knowledge and skill in the solution of codes. He was put in charge of the code work of Military Intelligence with two clerks as assistants. [8]

The work of encoding and decoding our own cables and telegrams [9] increased so rapidly, however, that although First Lieutenant James K. McKenna was soon appointed to take charge of this branch of the work, the time of the whole staff was practically consumed by it and Lieutenant Yardley had no opportunity to devote himself to code and cipher attack. Late in September therefore, Col. Van Deman invited to Washington and later commissioned as Captain, Mr. John M. Manly, [10] who had offered his services in March, 1917. At first it was Col. Van Deman's idea to divide the code and cipher work and put Lieut. Yardley in charge of the former and Capt. Manly in charge of the latter, but these officers soon saw that such a division would be counter to the best interests of the work and at their suggestion a section was organized to deal with secret communications of all sorts. Furthermore it soon became clear that such a section - to obtain the best possible results - should be located in Washington and should receive information and materials from all departments of the Government and serve all equally.

In pursuance of this plan Col. Van Deman had conferences with representatives of the departments of State and Justice and the Navy, and arrangements for cooperation were completed whereby these departments agreed to send to Military Intelligence all documents suspected of containing secret communications, and Military Intelligence agreed to examine and report upon such documents. Later, similar arrangements were perfected with the Postal Censorship; and even official and semi-official organizations with which no definite plan of cooperation had been arranged gradually adopted the practice of depending upon Military Intelligence for cryptographical work.

The Riverbank Laboratories.

Previous to these plans for cooperation and the organization of this central office, very little cryptographical material of any sort had been recognized as such by any department. A few official ciphers [11] were picked up from time to time and still fewer personal ciphers - innocent or criminal in character - drifted in from various sources. Most of these had been sent to

Geneva, Illinois, where, under the name of The Riverbank Laboratories, Mr. George Fabyan [12] maintained a staff of persons to work upon various fads in which he was interested. Among these fads was the belief in the existence of a biliteral cipher in various works of the sixteenth and seventeenth centuries which showed that Francis Bacon was the author of works commonly ascribed to William Shakespeare and other writers. The search for this cipher had given Mr. Fabyan's staff no real experience even in the elements of cryptography but had aroused in him an intense interest in the subject. Consequently when war was declared it was natural that Mr. Fabyan as a patriotic citizen should offer the services of this staff to the Government. This was in April, 1917. As no official cryptographic section then existed, Mr. Fabyan's generous offer was accepted and various departments of the Government sent to him such ciphers as came to hand. As has been said above, his staff was without real cryptographic experience, and to remedy this Mr. Fabyan sent two of them - Mr. J. A. Powell [13] and Mr. W. F. Friedman [14] - to the Army Service Schools at Fort Leavenworth to take a course of instruction from Lieut. Mauborgne; [15] consequently they were thereafter much better equipped to solve such problems as were submitted to them.

In the maintenance of his cipher laboratory and later in instructing a large number of officers in the principles of cipher attack, [16] Mr. Fabyan spent a large sum of money. For the assistance he rendered in these ways he deserved and received the thanks of the departments concerned. After the cryptographic section of Military Intelligence had been organized and designated as a central office serving all departments, however, relations with Mr. Fabyan's laboratory gradually ceased - on the part of the departments, chiefly because of the advantages of dealing with an office centrally located in Washington; on the part of the Military Intelligence because, in spite of repeated admonitions by Colonel Van Deman, Mr. Fabyan was unable or unwilling to suppress his penchant for a publicity which was recognized as detrimental to the best interests of the service. [17]

Code and Cipher Attack.

In the cryptographic section itself - which will hereafter for the sake of clearness, be referred to as M.I.8. - as in the whole organization of Military Intelligence, the increase in personnel was closely dependent upon the pressure of the work itself. During the first year of the war, additions to the staff were not made until they were absolutely necessary. The growth was therefore slow and the time of the staff fully occupied by current routine work. Plans for attack upon large problems or for research into new methods had constantly to be postponed because of the unescapable (sic) demands of the daily work. In fact, it was not until the beginning of August, 1918, that the

staff was enlarged sufficiently to permit of serious attacks upon the large numbers of code messages in various codes which had been accumulating in the files.

The results obtained should be judged in the light of these facts. And for the future it should be borne in mind that an adequate personnel of clerks and typists as well as of cryptographers is necessary for satisfactory results in code attack, and that the personnel is not adequate unless it is large enough to release the time of one or more experts for research.

Shorthand Subsection. [18]

The earliest subsection to be organized in M.I.8 was the Shorthand Subsection. Early in October, 1917, M.I.8 began to receive letters and other documents supposed by the censors to be in cipher. Some of them upon examination proved to be Yiddish and Arabic and were put into the hands of our language experts, but others proved to be in shorthand systems and languages of enemy countries and neutral European countries and in English shorthand systems unknown to most English shorthand writers.

In these circumstances recourse was had to Mr. F. W. Allen, of the firm of Hulse and Allen, who responded promptly with the desired aid and very soon was doing a large amount of work for M.I.8 and employing a number of experts and paying for their services connected with this work, until May, 1918, when he was requested to organize the work as a subsection of M.I.8, which he consented to do, without remuneration.

He was then appointed Chief of the Subsection, with the status of civilian volunteer and with headquarters at his office in New York. Under Mr. Allen's direction three important results were accomplished:-

- (1) Decipherment of Shorthand Systems. - A bibliography of works in public and private libraries in the United States on rare and foreign shorthand systems was compiled and a library was built up, for use in which all volumes that were needed were secured. Altogether fifty-four systems were studied and analyzed and the leading characteristics of each system were charted, so that in a short time experts could determine the system used in practically every document submitted and transcribe the stenographic notes into the language used.
- (2) German Shorthand Experts for the A.E.F. - On June 17, 1918, M.I.8 was instructed to locate, appoint and send to France fifteen expert stenographers who could take down verbatim examination of German prisoners of

war. The Committee on Classification of Personnel in the Army having failed to locate a single person so qualified, Mr. Allen was requested to organize the search; and after writing several thousand letters to individuals, shorthand schools and stenographic societies, he was able to recommend the required personnel and assure a steady, though not a large, supply of men qualified as desired.

- (3) Census of Foreign Stenographers. - In connection with the work described in the previous paragraphs, a census was made of shorthand writers throughout the United States writing foreign language systems, each of whom was carefully investigated and a record made of his history, citizenship, employment, connections and qualifications. This proved of great value in all phases of the work done by the Shorthand Subsection.
- (4) Expert Linguists for M.I.8 and the A.E.F - About July 1, 1918, as a result of the increasing pressure of work in M.I.8 and frequent calls from the American Expeditionary Forces, France, for officers with a thinking knowledge of German for codes and cipher work, Mr. Allen was requested to find, investigate and recommend six cryptographers and twelve candidates for commissions.

The persons whom he selected and recommended have been among the best qualified for our work, several having occupied executive positions in our own office and all of these officers who were sent to France having proved thoroughly efficient. Moreover, several of the officers whom he chose, in turn recommended strong, well-equipped men and women for various positions in France and the United States.

About August 15, a sudden call was made on M.I.8 for Army Field Clerks, with an intimate knowledge of the Russian people and language, to accompany the Intelligence Section of the American Expeditionary Forces to Siberia, and Mr. Allen, on three days' notice, furnished two qualified candidates.

Secret Inks.

That the enemy was using secret inks for some of his communications was known in a general way from a very early date. The first actual case that came to attention, however, seems to have been that of a letter written with invisible ink in Modern Greek and brought across the Mexican border in the shoe of an illiterate woman. This was developed by simple processes in M.I.8 but many suspicious documents did not yield to treatment. Information of general nature was obtained from the British and the French concerning German technique in this field, and after much correspondence M.I.8 was put in possession of all the knowledge of our allies in these three ways:

- (a) By a voluminous report transmitted through Captain J. A. Powell, who was sent abroad in December 1917 to establish liaison with our allies in all matters of this general nature.
- (b) By the visit to America at the expense of M.I.D. of Mr. S. E. Collins, one of the best of the British experts in the detection of secret inks.
- (c) By the visit of Captain Emmett K. Carver of M.I.8 to Great Britain and France for study in the laboratories there.

Correspondence and other preliminaries delayed for a painfully long time the establishment of a laboratory in M.I.8. This did not actually take place until the removal to 1330 F Street in July, 1918. The laboratory was, however, at this date able to function immediately in highest efficiency. Its record under Captain Carver - and in his absence, under Lt. A. J. McGrail [19] - is one of thorough equipment for any problem in its field and of great usefulness. On an average over 2000 letters per week were examined from July 1, 1918 to February 1, 1919.

Instruction in Code and Cipher Work.

Besides instructing Military Attaches and their assistants in the proper use of our own codes, M.I.8 was obliged to conduct courses of instruction for several groups of persons;

- (a) Officers and field clerks for M.I.8, for G-2, A-6, A.E.F., and for the corresponding section of the expedition to Vladivostok.
- (b) Intelligence Officers for duty at home and abroad.

One of the most interesting by-products of this instructional work was a treatise on the organization of the German Army, more accurate and comprehensive, it is believed, than any similar treatise in the possession of the Allies. This was prepared by a member of M.I.8 for use in instructing code-attack officers for the work at the front.

Code Compilation.

Shortly after the organization of M.I.8 it was learned that the Germans were reading confidential messages passing between Generals Pershing and Bliss and the Washington office. This was known to be due to the possession by the Germans of copies of the Army Code Book [20] of 1915, the only book available

for our use, and to the inadequacy of this book to resist attack under such conditions. Preparations were made for the compilation of a new and better book and a special subsection was organized under the leadership of Captain A. E. Prines for this purpose. This book [21] was completed on July 1, 1918, and would have served its purpose well for a long time but for the fact that other organizations of the Army which had been permitted to use the book misused it in such a way as to destroy its security. Work upon another book [22] - with certain improvements in plan - was begun immediately and under pressure of necessity was hastened to such a degree that the volume was ready for use when the Director of M.I.D. went to France, December 2, 1918.

Other notable achievements of this subsection were the following:

- (a) Two Geographical Codes, - In July, 1918, a cable from General Tasker H. Bliss requested that a "list of code words be gotten out for the geographical names of all that section of France in which operations are now taking place, or are likely to take place in the future, based on the French map having a scale of 1:100,000 feet." This cable was referred to the Director of Military Intelligence for action; work was immediately begun on the FRENCH GEOGRAPHICAL CODE, and the book of 360 pages, containing the names of approximately 9750 places in France within twenty-five miles of each side of the then battle front, was finished October 1.

By that time, since the theatre of military operations had materially shifted, it was considered desirable to issue a new code, incorporating the former, and also covering all of Belgium, the lower part of Holland, Germany to a distance of twenty-five miles beyond the Rhine, and that portion of Northern France not embraced in the former code. Work was begun October 17, and the book came from the printer about November 15, 1918. This code, FRENCH GEOGRAPHICAL CODE No. 2, contained approximately 26,500 names of cities, towns, forests, hills and streams.

- (b) A casualty code. - THE CASUALTY CODE, begun September 16, 1918, was in no sense of the word to be a secret code, but was designed purely to promote facility and economy in the transmission of casualty reports. In this work the War Department Telegraph Code of 1915 had been in use, but as it never had been designed for such a task, from five to seven or eight code groups were required to report a single casualty.

THE CASUALTY CODE was planned to comprise a long list of names, necessary numbers and dates, the name of every individual organization in the Army, including all branches, together with a number of provisional organizations contemplated at that time, and a vocabulary sufficient for the purpose for which the code was intended. The names, dates, numbers and

vocabulary were not especially difficult to compile, but when an effort was made to secure a complete list of organizations, it developed that no department in Washington had such a list. Considerable difficulty was therefore experienced in obtaining the information necessary, but it was obtained. Probably this section had in its possession on November 15 data with regard to the various branches of our Army, which, had it been properly tabulated, would have formed the most complete and comprehensive catalogue of our military resources in existence.

The work on this book was nearly completed, when the signing of the armistice, and the necessity for the immediate compilation and production of Code No. 9, rendered further work undesirable. The material gathered at that time, however, is still in the possession of M.I.8, and would be available if the publication of such a code ever became necessary.

- (c) Pocket code. - On the second of December, 1918, instructions were given to the Compilation Section to prepare a "pocket code," [23] for the use of Military Attaches when on duty away from their posts, and other special military agents in the field, particularly those agents who would go into enemy territory with the army of occupation or in other capacities in which the use of code communications was desirable. Within two weeks of the time when work was started the volumes were ready for distribution. The force had previously worked on the manuscript at odd times, and the devising of a new method of preparing the "copy" for the printer made possible this record speed. Fifty copies of the book were immediately sent to Europe for distribution, and those who have had occasion to use the book have been highly pleased. The book contains 13,000 code groups, words, and phrases.

In addition to code compilation, this subsection furnished new encipherment tables every two weeks to all users of our own codes and to such of our officers as were obliged by circumstances to continue the use of the Army Code Book of 1915.

Communications.

For two years the Communications Subsection has maintained cable and telegraphic communication with about forty Military Attaches and Intelligence Officers in Foreign countries, and with hundreds of Intelligence Officers stationed in all camps and important cities within the United States. The section has been open twenty-four hours a day. By means of special wire connections exceptionally fast service was provided, particularly with the most important center, Paris, whence cable messages were often received within less than one-half hour from the time of sending.

Practically half of the enormous amount of cable correspondence handled by this office was in the form of code messages. Since the principles of security required that the code words of each message be enciphered to prevent the possibility of the messages being read by the enemy, it was necessary to subject each code message to two complete translations. The obvious impossibility of distributing the work evenly according to clock or calendar resulted in intermittently overloading the section, but because of the splendid spirit shown by the entire commissioned and civilian personnel in subordinating their personal convenience to the needs to the work, and their willingness to "carry on," often for double the regular number of working hours, the work was kept up to the minute at all times and was always performed with exceptional efficiency.

From September, 1918 to May, 1919, this subsection sent and received 25,000 messages, about half plain text and half code, containing 1,300,000 words.

It is perhaps not generally recognized that our use of codes has resulted in great economy. Wherever they have been used, - and they have been used by the Military Intelligence Division, The Adjutant General's Office, the A. E. F., France, and other War Department offices, - the cost to the Government of cable and telegraphic communication has been reduced at least fifty per cent. The use of the Geographical Codes resulted in even greater economy by eliminating the necessity for spelling out foreign place names.

REFERENCES AND NOTES

1. The document of which this is a verbatim transcription is now filed in the office of the Director of Communications Research, Signal Security Agency (file no. 277). Though unsigned, proof exists that it was prepared by Major Herbert O. Yardley and completed probably in July 1919. The evidence for this attribution is now filed in IR 4150 and has been transcribed in The Shorthand Subsection of MI-8 in the First World War (1917-1919), a publication of the Historical Unit (IR 5042). On 3 June 1919 Major Yardley wrote Mr. Franklin W. Allen, who had been head of the Shorthand Subsection of MI-8 in New York, that, at the request of the Director of Military Intelligence, he was then preparing an account of the work of MI-8. He enclosed for Mr. Allen's comments and revision a rough draft of the fourth paragraph, dealing with the work of the Shorthand Subsection. This draft is reproduced in appendix A of the publication cited. Appendix B presents Mr. Allen's revisions. As appendix B has been incorporated almost verbatim in the unsigned document, it is clear that Major Yardley was the author.

2. The official title was "The Cipher Bureau."
3. Colonel Ralph H. Van Deman, General Staff Corps.
4. Brigadier General M. M. Macomb, War College Division, wrote on 2 August 1916 (file no. 4131-14, copy now in IR 4241) to the Chiefs of Staff of the Eastern, Central, Southern, Western, Hawaiian and Philippine Departments, that, in response to an earlier request for information, he had been sent by the Army Signal School, Fort Leavenworth, a list of officers known to be cipher experts. This list included Captain Parker Hitt, 19th Infantry, "undoubtedly the best cipher man in our service;" Lieutenant Joseph O. Mauborgne, 8th Infantry, who "has done some excellent work in this line and should be of value to the War College;" Lieutenant Charles A. Lewis, 9th Infantry; Lieutenant Edmund R. Andrews, 13th Infantry; Lieutenant Charles E. Swartz, 22nd Infantry; Lieutenant Clyde L. Eastman, 20th Infantry; Lieutenant Karl Truesdell, 25th Infantry; and Lieutenant Frank Moorman, 18th Infantry, who "is interested and would be glad to undertake work of this kind." The comment on Lieutenant Moorman was written by himself, as he was Acting Director of the Signal School at this time.
5. Colonel Hitt became Assistant Chief Signal Officer for the American Expeditionary Forces in France and was not actively engaged in cryptographic or cryptanalytic duties. (W.F.F.)
6. Lieutenant Colonel Moorman (then Major) was officer in charge of the unit (G-2, A-6) which performed cryptanalysis of German communications at General Headquarters, American Expeditionary Forces, France, 1917-1918.
7. Major General Joseph O. Mauborgne was Chief Signal Officer from 1 October 1937 to 30 September 1941, when he was retired.
8. This unit worked at the War College, but was later located successively in a building at 15th and M Streets, N.W., 1330 F Street, N.W., and finally at 7th and B Streets, N.W.
9. This purely cryptographic work should have been done by the Adjutant General's Office but on pleas of greater security G-2 set up its own facilities and staff for this purpose. (W.F.F.)
10. Both before and after the war Captain Manly was had of the English Department and Professor of English at the University of Chicago.
11. On such systems see IR 5049.

12. An honorary title, conferred by the Governor of Kentucky, some years before 1915, gave him the right to be known as "Colonel Fabyan." (W.F.F.)
13. Dr. Powell had been head of the University of Chicago Press up to the time of his employment in 1917 by Colonel Fabyan. (W.F.F.)
14. At that time Mr. Friedman was in charge of the Department of Genetics at Riverbank Laboratories and took only a mild interest in the Bacon-Shakespeare work being done there. (W.F.F.)
15. An error: Mr. Friedman was not sent but studied Captain Parker Hitt's Manual for the Solution of Military Ciphers, a copy of which Mr. Posell brought back with him. (W.F.F.)
16. A memorandum for the Chief of Staff from the Chief, Military Intelligence Division, General Staff, 13 May 1918 (a copy is now filed in IR 4152) stated that the officers sent to Riverbank Laboratories were sent there for training in cryptography but had been trained by error in cryptanalysis. On the other hand, when the student officers were detailed for the course, the War Department set up no guides or limitations, other than that six weeks would be devoted to instruction in cryptography. The word "cryptanalysis," coined by Mr. Friedman in 1921, was unknown at this time. Mr. Friedman recalls (1945) that there was some controversy with Major Yardley at a later time about this point, Yardley claiming that the officers had been sent for instruction purely in cryptography and not in solution. As it turned out, a great many of the students did get assigned to cryptanalytic duties. There were three groups of students, the first consisting of but four officers in October-November 1917; the second consisting of some sixty officers in January-February 1918; the third consisting of seven or eight in March-April 1918. Mr. Friedman prepared the instructional material, gave the lectures, and directed the school, the first of its kind in American history. Beginning in September 1917, Mr. Friedman gave up his work in genetics and became Director of the Department of Ciphers at the Laboratories, until in April or May 1918 he was commissioned first lieutenant and sent immediately to G-2, A-6, General Headquarters, in France. (W.F.F.)
17. No. This was just Yardley's way of getting Fabyan out of the picture. (W.F.F.)
18. This section is almost a verbatim copy of an earlier draft of these paragraphs, as revised by Mr. F. W. Allen. See the remarks in the Editor's Foreword.

19. Lieutenant Colonel A. J. McGrail was the only member of MI-8 in Washington who later also was a member of the Signal Security Agency in the Second World War. From 1941 until his death on 30 April 1945 Colonel McGrail was in charge of all work involving secret ink and photography.
20. War Department Telegraph Code 1915, a one-part code. It was used for unenciphered nonsecret communication, and with cipher tables for secret communication. The code itself had been printed by a commercial firm in Cleveland!! (W.F.F.)
21. Its designation was "Military Intelligence Code No. 5" but, so far as is known, there never were any similar codes numbered 1-4. (W.F.F.)
22. This two-part code was designated "Military Intelligence Code No. 9" and was little used. It was later revived with a new title-page as "War Department Staff Code No. 2," and held in reserve. It was probably never used.
23. The Ideal Correspondence Code, ostensibly a publication of the Ideal Code Company, New York, 1918, but actually printed at the Government Printing Office on paper and in a format unlike other government publications. (W.F.F.)



Really! I break codes!

BECAUSE OF THE FREEDOM OF INFORMATION ACT (FOIA)

LOUIS KRUH

[This column features documents which have been released by government agencies because of the FOIA request for a declassification review. Currently, intelligence agencies are lobbying for legislation which would exempt them from the provisions of the FOIA. Therefore, this column hopefully will serve two functions, (1) provide interesting material for your enjoyment and (2) make you aware of the FOIA process. Readers are encouraged to send us copies of material they have received through the FOIA, which they feel may be of interest to our readers.]

The following encrypted message, sent by the Mexican Consul in Yuma, Arizona, is 1920, was intercepted by the Military Intelligence Division, War Department and its decipherment/translation also follows.

These documents were requested under the FOIA in July, 1981. After the mandatory declassification review it was initially determined that classification must be extended until the year 2011. An appeal was made pursuant to the provisions of the FOIA and in January, 1982 the first reviewer was overruled and the material released.

If any reader solves the cipher system and sends a write-up to Editorial Office, CRYPTOLOGIA, Rose-Hulman Institute of Technology, Terre Haute IN 47803, we shall include it in a future column.

GENERAL CARLOS PLANK

MAGDALENA SON MEX VIA NOG JCT

ARAIZA DICEME TRANSCRIBA A UN SIGUIER MENSAJE QUE AYER A LAS SIETE Y MEDIA
 DE LA MANANA 09 45 32 19 06 03 47 26 78 45 94 QUE PUEETE COMPROBAR ESTA 15 63
 07 19 06 10 40 54 60 03 18 56 17 80 93 51 09 34 06 52 14 94 26 15 63 40 39 36
 78 47 49 03 34 84 18 56 45 51 56 55 19 36 07 71 80 18 46 07 09 02 23 18 03
 07 23 45 08 19 06 65 15 02 35 66 50 19 COMO TRES NILTAS 19 45 08 36 06 49 40
 08 66 69 60 94 84 07 51 15 06 19 21 40 94 54 POR DOS VECES CONCECUTIVAS 17 5
 65 10 23 07 60 15 26 56 66 33 41 86 08 03 22 32 17 36 06 03 33 70 19 59 27
 17 69 66 02 19 07 YENIA 15 06 64 80 18 46 55 19 32 92 36 51 02 32 63 42 15
 03 06 08 16 66 92 01 78 50 19 40 66 15 26 80 01 16 06 40 17 32 INFORMES SUMIT
 ADE POR 01 23 43 60 08 18 06 36 07 80 44 36 06 23 82 15 02 45 07 05 52 19 06
 24 50 21 09 15 49 35 80 93 26 78 20 49 93 08 19 69 15 ME HACEN SABER QUE
 08 49 15 23 80 18 60 40 36 43 32 23 66 65 07 09 19 50 51 56 14 32 06 15 26 56
 63 84 43 46 15 26 80 63 40 45 19 15 18 85 10 40 50 03 49 40 15 CRELLENDOS
 HAYA SIDO 78 18 48 52 23 06 40 35 46 RECIENIENTEMENTE POR 01 19 16 36 26 33 56
 07 DADO QUE SE DIFERENCIA 19 45 34 03 26 66 69 13 94 06 49 46 07 35 19 06 32
 26 63 84 50 A LAS QUE ANTERIORMENTE 22 32 65 10 19 06 60 57 23 22 43 15 56 27
 52 84 26 94 07 CON EL MIGMO OBJETO COMPEDBADO QUE 06 19 23 45 32 22 16 60 4
 83 66 17 94 01 40 79 60 66 93 02 18 03 Y A SU VES 22 15 02 49 01 16 38 35
 15 10 78 49 23 03 07 40 02 18 23 27 30 35 09 03 07 PARA QUE 19 02 10
 93 19 02 78 21 52 15 24 36 50 56 65 EL DISTRITO DE ALTAR CON ESPECIAL
 17 56 06 34 15 02 46 50 78 43 80 53 03 26 07 70 22 56 08 03 01 15 35 4
 84 17 80 09 17 23 03 45 19 07 A FIN DE QUE 34 43 26 09 01 45 80 QUE 1
 26 43 19 21 32 06 02 94 07 52 20 06 15 26 57 07 18 15 02 45 50 CONSIG
 Y SE 15 15 78 26 40 14 80 06 32 EL CONTENIDO DE 26 08 50 32 32 09 15 24 1
 DE CUE TIENE QUE 39 15 54 26 06 52 07 49 RESPECTUDSAMENTE

CONSUL ALEVANDRO VANARIENEZ

Refer: Intercept-Nogales

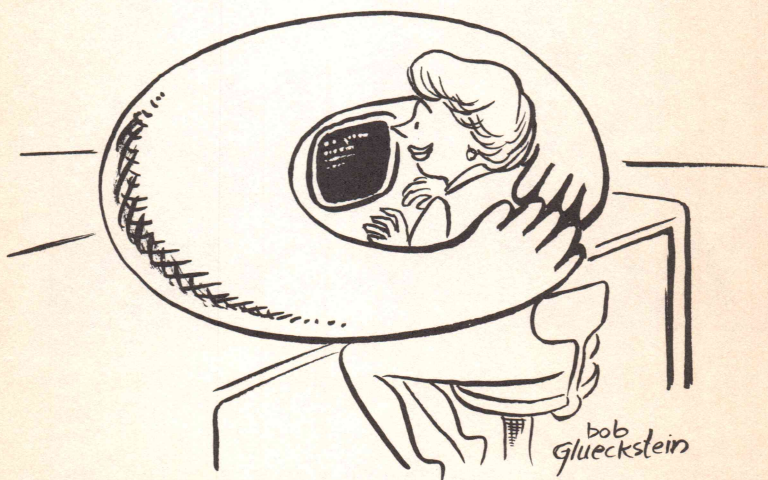
Aug. 18 1920

From: A.V. Martinez
Mexican Consul
Yuma, Arizona

To: Gen. Carlos Plank
Magdalena, Son.

Araiza asked me to transcribe the following message: At 7:30 a.m. yesterday, an aeroplane in the service of Cantu- as can be proved- coming from the United States, flew twice in succession over the dividing line, penetrating about three miles into the interior of this territory, evidently for the purpose of making observations. It was equipped with a machine gun, bombs and wireless. Through information received from American military men who are patrolling the border, I learned that it flew in a southeasterly direction, parallel with the dividing line. I believe this plane was purchased recently by the rebels in view of the fact that it is different in color from those which up to date have made flights here for the same purpose. It has also been proved that Reina has been instructed and in turn for this purpose has appointed several individuals to poison the watering places in the district of Altar and especially those near "La Bolsa". I have taken the proper precautions to prevent the column about to arrive from suffering any harm and I am having the water of all watering places which they will use first analyzed.

A.V. Martinez



"Feel secure with this encipherment unit--"

CIPHER DEVICES

LOUIS KRUH

When Jim Gillogly went on vacation to London in May 1979, I suggested that the cipher machines in the Science Museum were worth a visit. Serendipitously, he got in touch with the Museum's Telecommunication Section instead of the Math Section where the machines I had in mind were located. As a result, the Telecommunication people showed him their Autocryptograph, which has apparently languished there unknown to anyone outside of the museum (and to many inside the museum, too) for over 50 years.

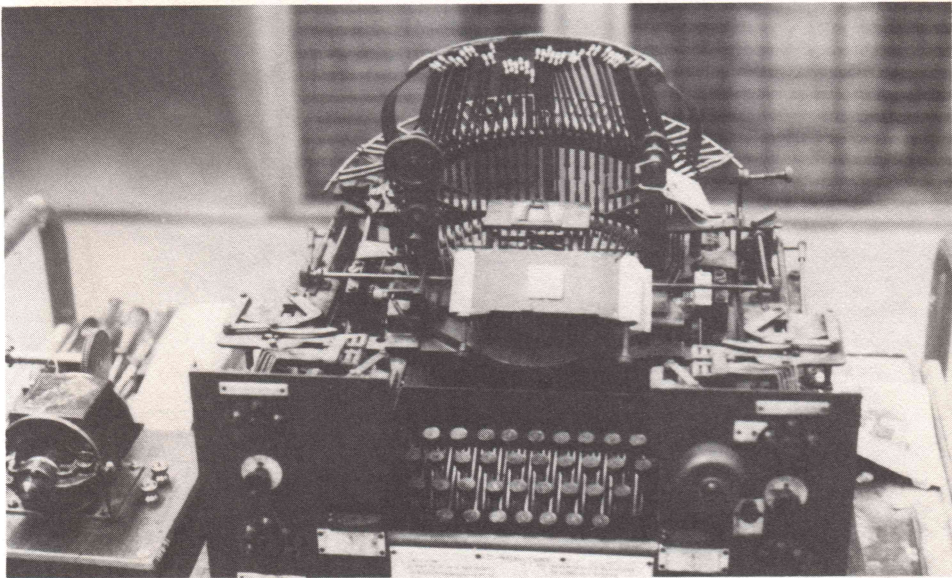


Figure 1. The Autocryptograph.

Jim took photographs of the machine and wrote a brief description of it. Subsequently, I alerted Donald W. Davies to the existence of the Autocryptograph. Mr. Davies has been examining cipher devices and machines in London museums and preparing sketches and extensive descriptions of them. After

locating the machine, which was not a simple task unless you got to the proper section, he made a series of drawings of its mechanism and developed a comprehensive paper on how it worked.

Both Gillogly's and Davies' descriptions follow. Davies, who lives in England, obviously was able to spend more time with the Autocryptograph. Gillogly's paper includes a cipher prepared on the machine. Let us know if you solve it or if you know of any information about the Autocryptograph.

THE MYSTERIOUS AUTOCRYPTOGRAPH

JAMES J. GILLOGLY

Almost forgotten in the Annex of the Science Museum in London lies a lovely old electromechanical cipher machine called the Autocryptograph (Figure 1). In 1928 the War Department donated it with blueprints to the Science Museum, which gave it the identification number 1928-91. The curator thought the machine had been used during the first World War, but he had no direct evidence to support his guess. I was allowed to take pictures and to play with the mechanism, but did not have a power source that was likely to operate the motor. The Autocryptograph is well-preserved, with no frozen fears or levers, and it looks like little work would be required to make it work.

The QWERTYUIOP keyboard includes a space bar, the digits 2 through 9, and a special key with three A's around it. Each side has controls for setting "Encipher", "Clear", and "Decipher".

The Autocryptograph apparently combines substitution and transposition. The controls include a "right transposer" and "left transposer", each with a red knob marked "SET" and four black ones with settings 1-5. Figure 2 shows the mechanism of the right transposer, which adjusts five "pallet-bars".

The "right substitutor" and "left substitutor" control the position of Vails with lugs. Each of the seven substitutor knobs (one red) controls a Vail in the cage-like cylinder shown in Figure 3.

The remaining control is a dial numbered 0-18 just below the right transposer controls. It may control the nearby bell.

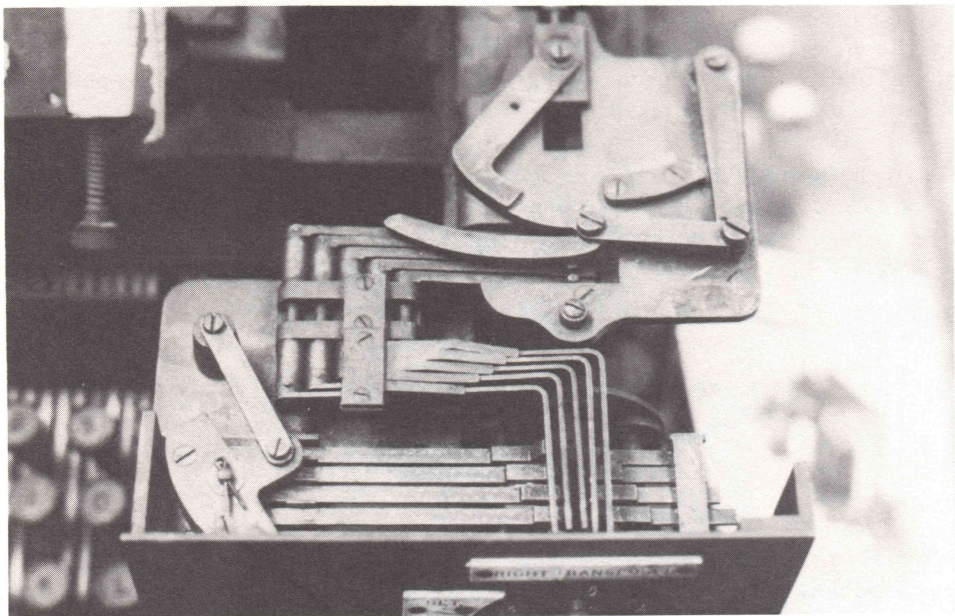


Figure 2. Mechanism of the right transposer.

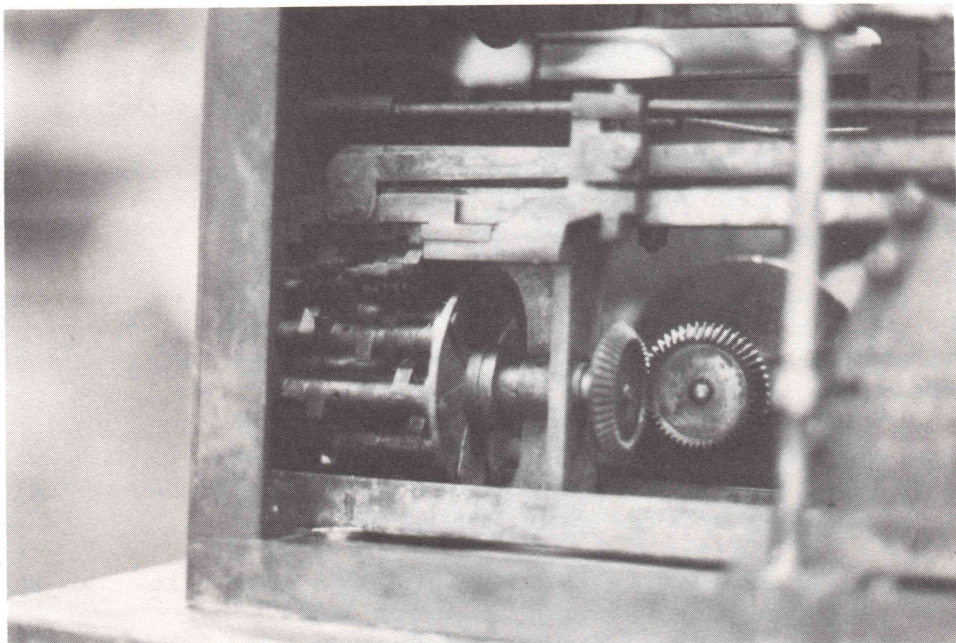


Figure 3. Mechanism of the right substitutor.

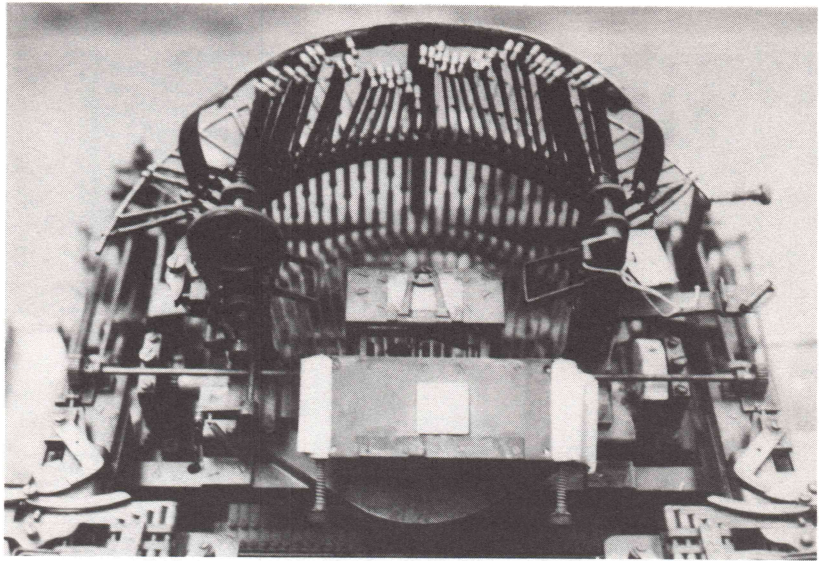


Figure 4. Basket and paper rollers.

There is some hope for identifying the algorithm without sending someone who can read the blueprints which are available. Stored with the Autocryptograph was a fat wad of coding forms with the designation "Army form C2130". Each was a strip of separate 5 x 5 blocks. All but one of the forms was blank. On that form (in a work holder above the keyboard) was written in pencil the following cryptogram:

QR07K	PKRLG	D3VAI	RKD3F
TYPJC	29RIL	KGXSU	243TY
PAXMV	XC9PO	2ECEP	KEQD9
RWHLB	NW3G1	P44CZ	L84MC
KUW5E	FTJXU	9UA3P	SDKWJ

This is not very much data, but it may be adequate if it turns out to be one of the standard stilted messages used for demonstrating cipher machines.

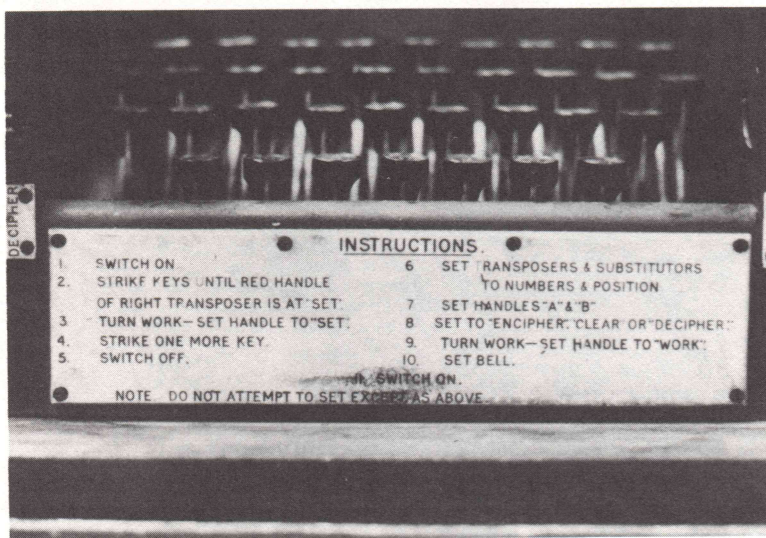


Figure 5. Instruction plate.

THE AUTOCRYPTOGRAPH

DONALD W. DAVIES

This machine was given by the War Office to the Science Museum in 1928 or 1929. The only clues to its origin are on the forms supplied with it. These words are, on different ends of the same strip of paper:—

Army form C2130, For use with Autocryptograph.
Form "Sigs Exp^{tl} Est. P. No. 9257".

We can guess that this was an experimental model under trial and that the design was abandoned. It is very well designed and made but the mechanism is rather light in construction. It is also complex and has few adjustments for mechanical tolerances so that it was probably unsuited to army use.

It has been coated with a preservative sticky grease which makes it impossible to operate the mechanism as a whole, though enough pieces can be moved to enable most of its functions to be deduced. There is a connecting drive shaft at the back, with a magnetic clutch, and a separate electric motor with worm-gear reduction.

It has two subsystems with common drive shafts but functionally separate. Generally the 'substitution machine' is placed at the bottom and the simpler 'transposition machine' at the top of the mechanism.

The Substitution Machine.

The keyboard has 35 keys. The key which is depressed generates a code of two 'digits', 1 out of 5 on the left side of the machine (a quinary digit) and 1 out of 7 on the right side of the machine. Each digit is separately enciphered, as we shall describe later. This encipherment is a polyalphabetic substitution repeating after $17 \times 6 = 102$ characters for the left hand, or quinary digit and $19 \times 7 = 133$ characters for right hand, or 7-ary digit. The resulting code with a range of 7×5 values operates the type bars, selecting one out of 35 printed characters.

The character set is ABZ, 2, 3, 4, 5, 6, 7, 8, 9 and a key marked AAA. We did not find out how either the keyboard or the printed characters correspond to the 7×5 code.

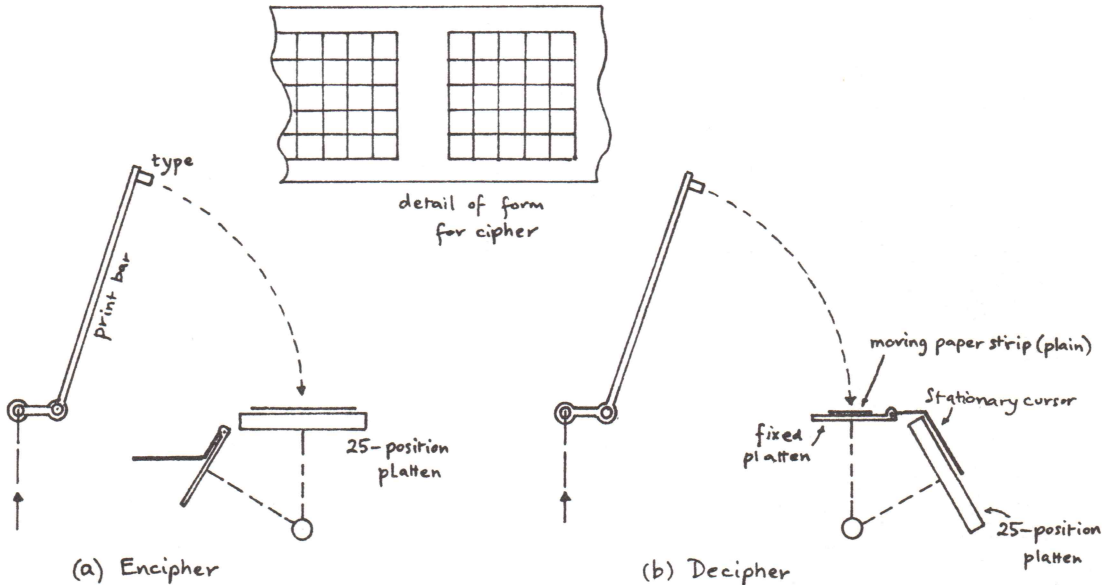


Figure 1.

The transposition machine

The printing arrangements are altered by moving two platens, backward for encipherment and forward for decipherment. For encipherment (Figure 1a), the type bars strike on a platen holding a printed strip with a 5 x 5 matrix of cells on it. The platen moves 'pseudo-randomly' to 25 different positions in successive strikes, generating a transposition of this 25-character block. We can assume (since vertical movements are more frequent than horizontal) that the cipher is read off in normal L-R, top to bottom, reading sequence for serial transmission.

For decipherment (Figure 1b), the platens are moved forward. The type bars then strike on a fixed platen, where there was, it seems, a paper tape feed and an inked ribbon feed. The movable platen moves into the same 25 places in turn, as before and takes with it the attached message form, with its message in the 5 x 5 matrix. A cursor rests on the form, indicating to the operator which character is to be read next and keyed.

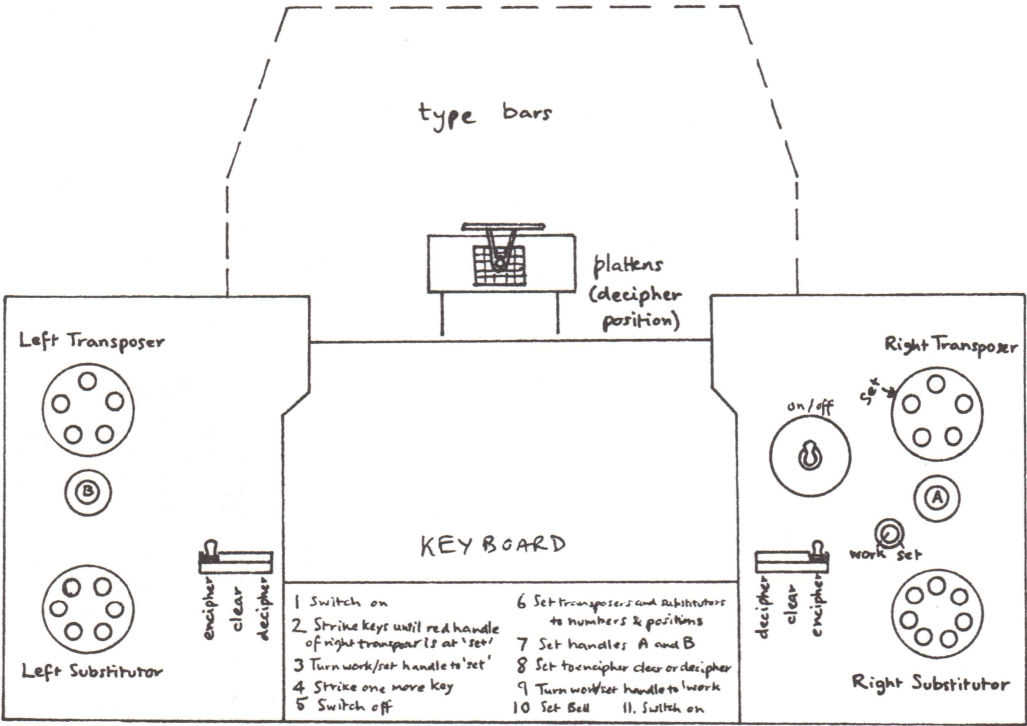


Figure 2(a).

Combined effect

It will be seen that the substitution (which is not an involution) must be switched to encipherment or decipherment. There are two control levers for this purpose. The transposition movement is the same for encipherment and decipherment.

Encipherment is a character substitution followed by the transposition of a block of 25 characters.

Decipherment is the inverse transposition followed by the inverse substitution. The inverse transposition is obtained by reading from a cursor which indicates the same sequence as that in which the characters were printed.

The cipher as a whole repeats after $102 \times 133 \times 25 = 339,150$ characters.

The transposition machine in detail

Figure 2a shows the front panel and the controls and settings. Figure 2b details the instructions. At the left and right of the panel at the top are two turrets, each with 5 positions. In the turrets are 5 small camshafts, set by turning small setting 'handles' on the front panel. They are set to a transposition, i.e. each camshaft of a turret is set to a different value. As the turret rotates, successive camshafts come into play. Each camshaft lifts one of five transverse bars, which convey quinary output digits. Figure 4 shows a similar mechanism, in part.

INSTRUCTIONS

- | | |
|--------------------------------|--------------------------------------|
| 1. SWITCH ON | 6. SET TRANSPOSERS AND SUBSTITUTORS |
| 2. STRIKE UNTIL RED HANDLE OF | TO NUMBERS AND POSITION |
| RIGHT TRANSPOSER IS AT SET | 7. SET HANDLES A AND B |
| 3. TURN WORK-SET HANDLE TO SET | 8. SET TO ENCIPHER CLEAR OR DECIPHER |
| 4. STRIKE ONE MORE KEY | 9. TURN WORK-SET HANDLE TO WORK |
| 5. SWITCH OFF | 10. SET BELL |
| | 11. SWITCH ON |

NOTE: DO NOT ATTEMPT TO SET EXCEPT AS ABOVE

FIGURE 2(b).

The right hand turret or 'transposer' moves once per character, while the left hand transposer moves every 5 characters - we did not trace enough of the drive mechanism to be sure of this. Each transposer generates repeatedly a permutation of the digit values 0, 1, 2, 3, 4.

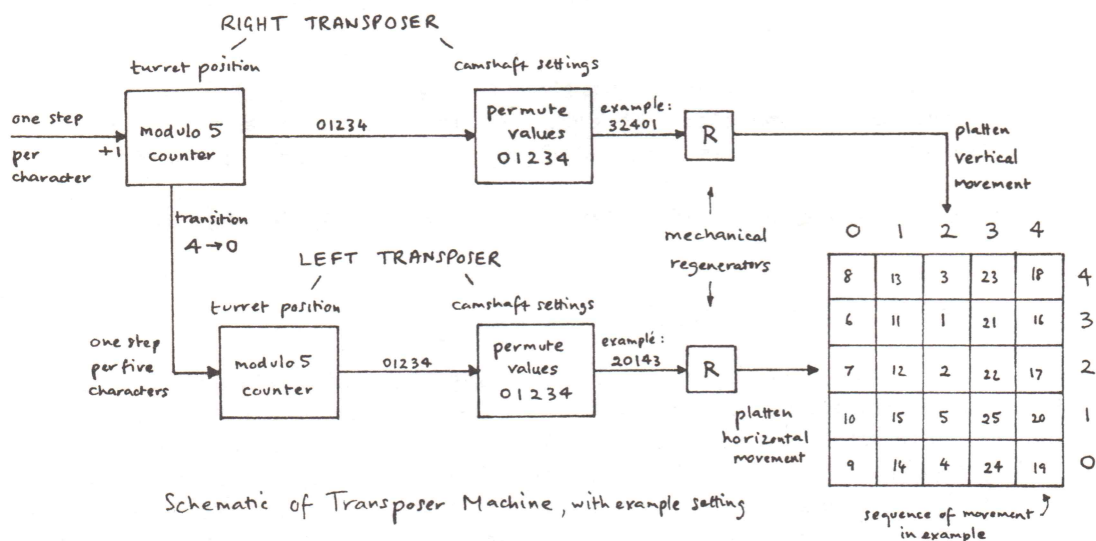


Figure 3.

When the bars are lifted, through a complex mechanism, one of 5 pins is lifted. A hook-shaped cam slides across, moving the carriage on which it is pivoted to a corresponding position. This is an example of a mechanical 'regenerator' or power amplifier, of which there are at least 3 pairs in the machine. The carriage movement, via a rack and pinion and various gears sets the platen movement, vertically from right transposer horizontally from the left transposer.

Figure 3 shows this schematically. The platen moves according to the vertical transposition for five moves, then takes up the next horizontal position and repeats the same vertical scan. After 25 movements a bell rings to remind the operator that the paper form must be moved on, ready for the next block. It does not have to begin the 25 character block at the start of 5 vertical positions, since before it finishes the 25 block it will complete the column on which it started.

The significance of the 'work-set' handle was not evident. It operates a contact, and may perhaps stop the mechanism in half-way position with the right hand transposer free to be turned. Normally this is the only one among the four turrets that cannot be turned.

The transposition machine contributes a factor of 25 to the length of message that occurs before the entire cipher repeats. The initial turret positions are therefore part of the 'message key'.

The turret settings, each a permutation of the 5 values 0, 1, 2, 3, 4, form part of 'basic key'. For the right hand transposer there is a natural datum point for the settings - the camshaft that is in the operating position at the start of the transposition of one column. For the left hand transposer, any settings that differ only by a rotary shift of the cam values give no essential difference to the encipherment pattern. Different message keys will make them equivalent. Therefore there are only $4!$ essentially different settings for this turret. The contribution of these settings to the basic key is $2800 = 5! \times 4!$

The substitution machine in detail

There is a lower left hand turret, the left substitutor, with 6 positions. Each cam has 5 settings, corresponding to the output values 0, 1, 2, 3, 4. We shall see, later on, that the range of values -2, -1, 0, 1, 2 probably gives a more convenient representation. We can conjecture that all 5 values should be represented somewhere on the turret, so there will be $15 \times 5! = 1800$ settings. If, however, the starting position is part of the message key, there are only 300 essentially different basic key settings on this turret, those related by rotation of the turret being equivalent. This turret moves on one position for each character enciphered, we believe. Figure 4 illustrates the substitution machine as a whole.

Between the two left hand turrets on the front panel is the 'handle B' which can be set to any of 17 positions 0-16. This sets the initial state of a cam which, moving once per character, we believe, generates a binary output that can be characterised as 110101010101010. The position of the double 1 in the scale 0-16 was not determined and the 0-1 notation is arbitrary.

We could not see how the cam and turret outputs were combined, but it seemed to be a 'linear' set of levers. These levers also formed part of a regenerator and the output was a 7 position movement. We conjecture that the cam output adds one (or not) to the turret output.

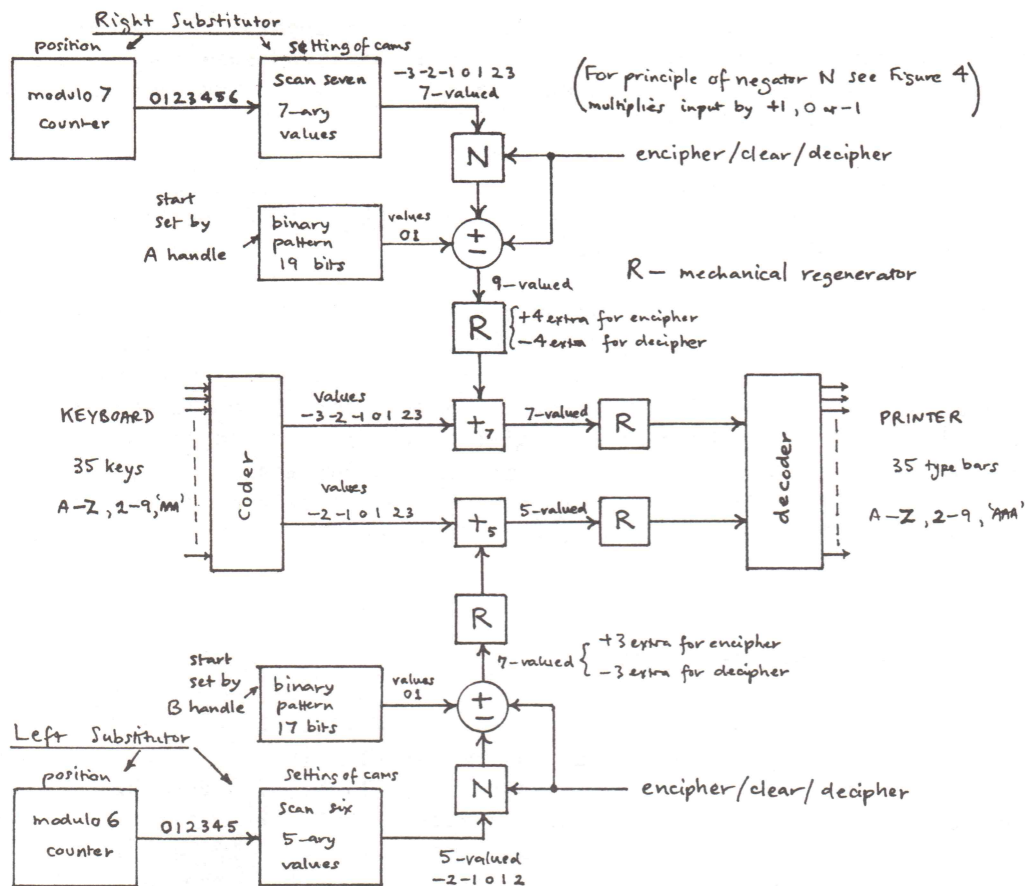


Figure 4.

For the purpose of encipherment and decipherment, the quinary output of the substitutor must be capable of negation, that is to say X is converted to $-X$. This is done by an ingenious mechanism in which 5 raised pins lie along a diagonal line of intersection of 5 bars with 5 bars at right angles. The lower bars (moved by the turret cams) raise the upper bars by their pins. A bar, to which all the lower bars are hinged, swings the lower bars to take up either diagonal position. Figure 5 shows the principle but is not an accurate picture.

Such a negation mechanism is fitted to all four turrets, but those involved in transposition have the diagonal bar fixed. The fact that a mechanism is provided in the transposition chain just for this purpose gives rise to a conjecture that negation controlled by the encipher-decipher switches was at

first applied to the transposition machine and then immobilized later. If cursor rather than platen movement had been used in decipherment it would have been needed.

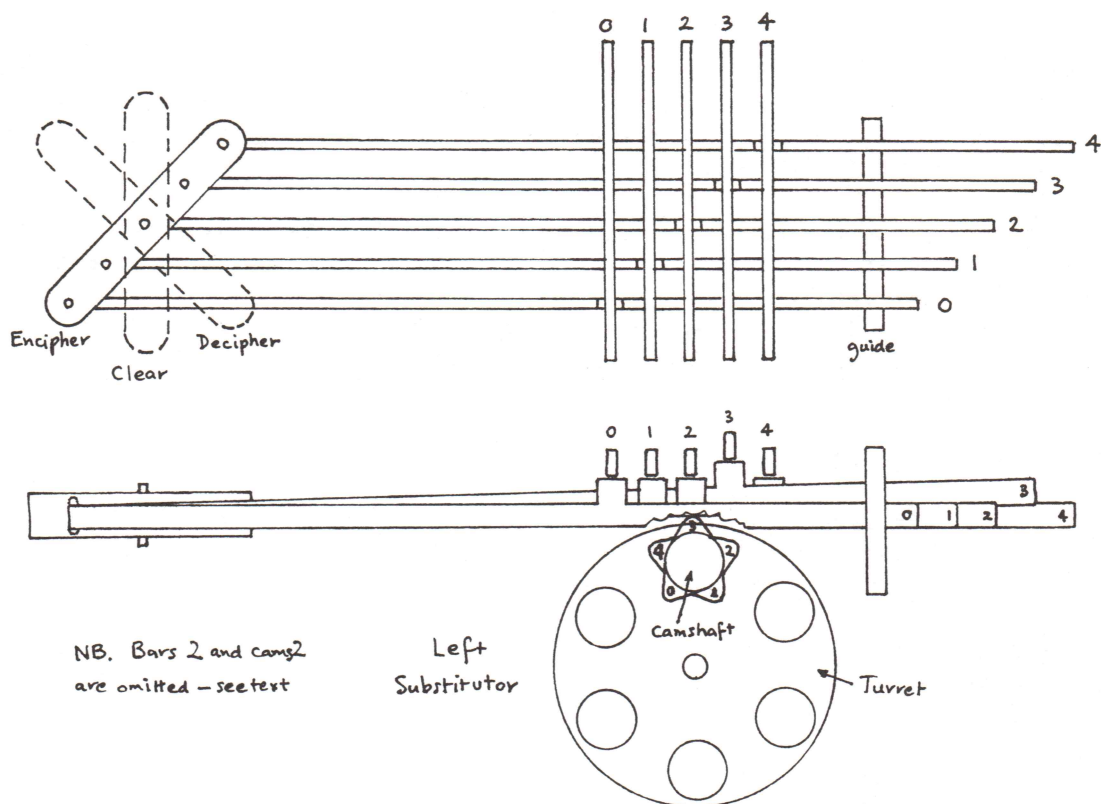


Figure 5.

The binary output of the 17 position cam, if it adds one to the values 0-4 during encipherment, must subtract one during decipherment. We did not find this mechanism but it is logically necessary and it would account for the fact that the eventual output has 7 possible positions (-3, -2, -1, 0, 1, 2, 3).

The 7 valued output is regenerated and used to position a carriage at the back of the machine which places 5 bars over a pattern of raised pins on bars coded by the keyboard which cross them. By this mechanism a modulo 5 addition is

done. The resulting output is again regenerated by the largest of the regenerators. The 4 regenerators in the substitution machine use floating jaws to close around a raised pin and clamp an output pin into the same position. The regenerated output of the adder drives part of the decoder for printing which is described later.

The right hand side of the substitution mechanism works in an exactly corresponding matter. The 7 position turret moves once for each character. Assuming the camshafts are all set to different values, there are $7!$ settings, but if turret initial position is used as part of the message key, there are $6! = 720$ essentially different settings.

The 'handle A' on the right hand side sets initially a 19 position cam. The binary sequence it generates has the form 11010101010101010. The negation and $+1$, -1 operations are as for the other side, and result in a 9 position output which is added to the keyboard input, modulo 7. The result is regenerated to operate part of the decoder for printing.

Size of the Basic and Message Key Space

Basic Key:	transposition left 4!	right 5!
	substitution* left 300	right 720
	combined effect: 622,080,000	

*These values depend on the assumption that all values of cam settings are used in each case.

Message Key:	transposition left 5	right 5
	substitution left 6	right 7
	handles B left 17	A right 19

combined effect: 339,150, the repetition period.

These numbers do not, of course give a good idea of the security of the cipher. Each of the cycles used in encipherment has a relatively small period (5, 25, 6, 7, 17, 19). Typically the difficulty of breaking such a cipher is related to the sum of these numbers, not their product.

The Clear Setting

We spoke of the substitution turrets as though the left hand one had 5 output bars and the right hand one had 7. In fact, the middle cam position on each

camshaft in these turrets is missing and so is the middle bar of the output. A simple mechanism (one part and a spring) is provided so that if no pin is presented to the regenerator by the 4 or 6 bars actually present, an 'extra pin' moves into place in the centre position.

This feature comes into operation in the 'clear' position of the encipher-clear-decipher levers. Figure 5 shows the effect of this setting on the negators. All the raised tags of the lateral bars impinge on the middle bar (called 2 in the figure) of the output. In the actual machine this is missing, but the end effect is the same, with the 'extra pin' taking its place. Since the effect required in the adders in the 'clear' condition is to add zero, we can see that a better way of labelling these outputs would have been as -2, -1, 0, 1, 2. This is the labelling used in Figure 5.

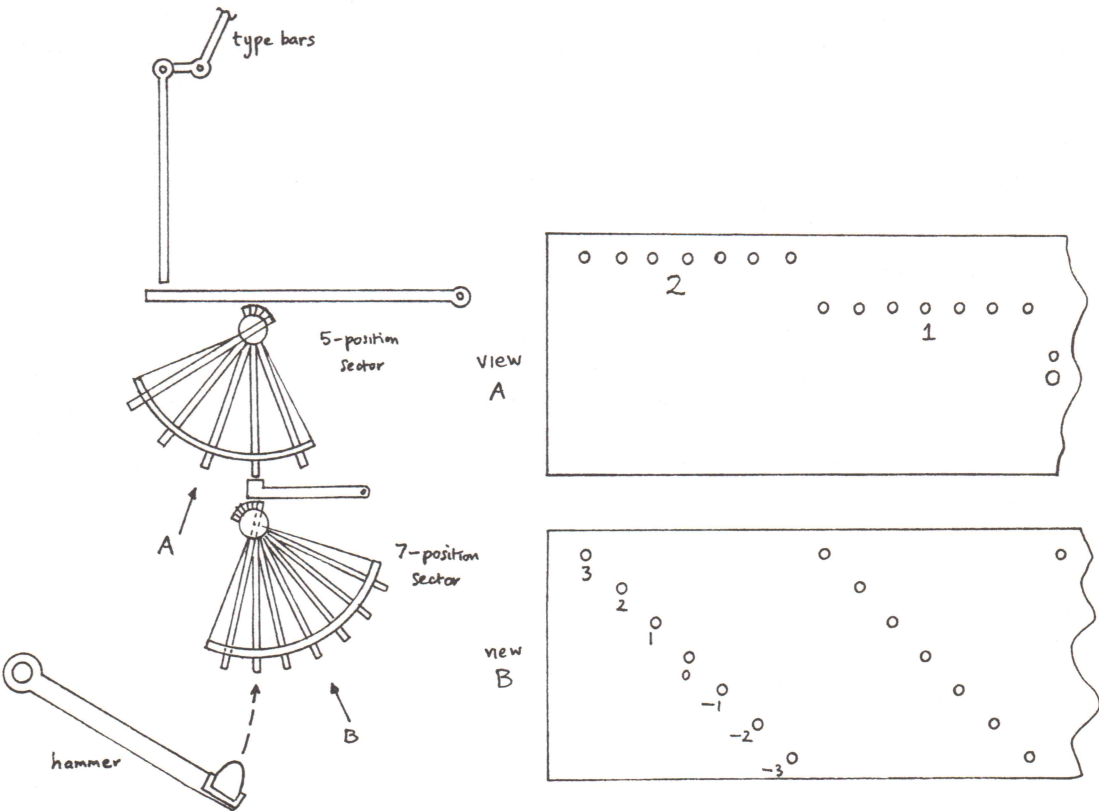


Figure 6. Principle of decoder-printer.

The Printer Mechanism

The output of the modulo 5 addition raises a pin which is the input to a large mechanical regenerator. The right side, modulo 7 is similar. The two regenerators each rotate a sector of a cylinder occupying the middle of the machine. Figure 6 shows the principle. Each sector has 35 rods running through it. The effect is to bring two of these rods into line in one of 35 longitudinal positions. A wide hammer with a rubber striker then pushes up the rods and moves one of the type bars. The array is regular in 5 groups of 7 bars across the machine, but the coding of the 35 printed characters was not examined, nor was the coding of the keyboard input, which should be the same, to allow for the 'clear' setting of the machine.

General Remarks

There may well be details of the mechanism and its operation that we were not able to discover, but the basic principles are in essence those described here. One of the unexplained features is the presence of 3 or more differential gears. These give the impression that some shaft movements are occasionally stopped or reversed. This might be another kind of complexity we did not discover. The effect of the 17 and 19 position cams was deduced from rather little evidence.

The principle of compounding a substitution and a permutation using two separate mechanical subsystems is ingenious. The mechanisms are very cleverly designed and neatly packed into the space. The preservative wax prevented any realistic test, but the lightness of the parts and the weak return springs imply that everything should be freely moving in a working machine. We had the impression that the machine would not be rugged and reliable. It would be very interesting to clean off the wax and give it a real trial. Then the remaining details of the mechanism could be discovered, in particular the sequence in which things happen.

BIOGRAPHIES OF CONTRIBUTORS

Donald Davies is a scientist at the UK National Physical Laboratory working on matters of data security and authentication. He began to work with digital computers in 1947, helping to build an early machine and then using it for traffic simulation and other studies. By 1965 he had moved to computer networks and developed an early packet switched network (he coined the word "packet"). Eventually this work led to a "distinguished fellowship" of the British Computer Society. Now his professional interests include the DES, public key systems and protocols for their use and his private interests include historic cipher machines. Address: Division of Information Technology and Computing, National Physical Laboratory, Teddington Middlesex TW11 0LW, England.

James J. Gillogly specializes in Artificial Intelligence at the Rand Corporation. He received his PhD degree in Computer Science from Carnegie-Mellon University. His professional interests include analysis of algorithms, game programming, and pseudo-random number generation. His formless interests in cryptography crystallized when he read David Kahn's The Codebreakers in the late 1960's. Since then he has spent a great deal of time with the Voynich Ms and has written programs to solve or help solve many of the ciphers used by the American Cryptogram Association. Address: 2520 Chard Road, Topanga CA 90290.

Gustavus J. Simmons is manager of the Applied Mathematics Department at the Sandia National Laboratories in Albuquerque NM. Sandia is the largest of the U.S. National Laboratories with the primary mission of systems engineering for the nonnuclear portions of nuclear weapons. Prior to this assignment, he headed a Division at Sandia that had primary responsibility for the design and evaluation of command and control systems for U.S. nuclear weapons. He received his PhD in mathematics from the University of New Mexico where his thesis research was on combinatorial designs. His research has been primarily in the areas of combinatorics and graph theory and in the applied topics of information theory and cryptography, especially as applied to message authentication and systems design to achieve this function. He has published extensively on both the theory and application of asymmetric encryption/decryption and on the authentication channel which he first formulated as a game theoretic model and has since developed into a general mathematical model.

Authentication systems have already been fielded by the Sandia National Laboratories, based on some of the results of his research, for such diverse applications as nuclear weapons test ban treaty verification, individual identity certification and reactor monitoring for the International Atomic Energy Agency. Address: Applied Mathematics Department 5640, Sandia National Laboratories, Albuquerque NM 87185.

Arthur Sorkin received his PhD degree in computer science from UCLA and the MA degree in mathematics from UC, San Diego. He is currently employed at Lawrence Livermore National Laboratory, where he has been engaged in research in computer security and parallel computing. Dr. Sorkin is also a lecturer in the Department of Applied Science, UC Davis/Livermore, where his courses include computer security and cryptography. Address: Lawrence Livermore Laboratory L60, University of California, P O BOX 808, Livermore CA 94550.

Greg Mellen is a staff engineer in the Sperry Univac Civilian Agency Systems Engineering Department. His interest in ciphers and language date back to his training as a classicist and his work as a cryptanalyst. Address: 8441 Morris Circle, Bloomington MN 55437.

Louis Kruh is a public relations executive with the Bell System in New York City. His interests in cryptology span more than forty years. He collects crypto material and machines. He has a BBA, cum laude, from the City College of New York, and an MBA, with distinction from Pace University. Currently he is nearing completion of law school. Address: 17 Alfred Road West, Merrick NY 11566.

David Kahn is an Editor with at least two hats. Besides his Editorship of CRYPTOLOGIA he is the Op-Ed Editor for Newsday, a large daily newspaper in Long Island, NY. In addition he continues his careful scholarship pursuits with publications in a variety of journals. Address: 120 Wooleys Lane, Great Neck NY 11023.

CRYPTOLOGIA FOURTH ANNUAL
UNDERGRADUATE PAPER COMPETITION
IN CRYPTOLOGY

WE ANNOUNCE THIS CONTEST TO ENCOURAGE THE STUDY OF ALL
ASPECTS OF CRYPTOLOGY IN THE UNDERGRADUATE CURRICULA.

FIRST PRIZE: THREE HUNDRED DOLLARS

CLOSING DATE: 1 JANUARY 1985

TOPIC MAY BE IN ANY AREA OF CRYPTOLOGY
TECHNICAL, HISTORICAL, AND LITERARY SUBJECTS

PAPERS MUST BE NO MORE THAN 20 TYPEWRITTEN PAGES IN
LENGTH, DOUBLE SPACED AND FULLY REFERENCED. FOUR
COPIES MUST BE SUBMITTED. AUTHORS SHOULD KEEP ONE
COPY. PAPERS ARE TO BE ORIGINAL WORKS WHICH HAVE NOT
BEEN PUBLISHED PREVIOUSLY. COPIES BECOME THE PROPERTY
OF CRYPTOLOGIA AND CRYPTOLOGIA ASSUMES ALL RIGHTS.

THE PAPERS WILL BE JUDGED BY THE CRYPTOLOGIA EDITORS
AND THE WINNER WILL BE ANNOUNCED ON 1 APRIL 1985 WITH
PUBLICATION OF THE WINNING PAPER IN THE JULY 1985
ISSUE OF CRYPTOLOGIA.

THE COMPETITION IS UNDERWRITTEN BY A GENEROUS GIFT
FROM BOSHRA H. MAKAR, PROFESSOR OF MATHEMATICS,
SAINT PETER'S COLLEGE, JERSEY CITY, NEW JERSEY.

INQUIRES, SUBMISSIONS AND SUBSCRIPTION INFORMATION:

CRYPTOLOGIA, EDITORIAL OFFICE
ROSE HULMAN INSTITUTE OF TECHNOLOGY
TERRE HAUTE, INDIANA 47803

COLLEGIATE MICROCOMPUTER - A NEW JOURNAL

COLLEGIATE MICROCOMPUTER is a unique forum for the exchange of ideas about the roles of microcomputers in higher education.

COLLEGIATE MICROCOMPUTER discusses uses of microcomputers in teaching and research, in classroom and laboratory, in library, studio, and office, in planning and development.

COLLEGIATE MICROCOMPUTER features the microcomputer in

- reviews and accounts of hardware and software
- descriptions of topics and courses
- results of research and experiments
 - presentations of student projects
 - experiences with consulting and workshops
 - uses in office work and material preparation
 - descriptions of extracurricular activities
 - reviews of peripherals, products, services, and literature.

COLLEGIATE MICROCOMPUTER represents the microcomputer interests of all college and university professionals and is a forum for your ideas, papers, opinions and announcements

Annual Subscription Rates: \$28.00 for US, \$36.00 for non-US, \$60.00 for non-US AIR MAIL

An annual volume includes February, May, August and November issues. Volume I, Number 1 is February 1983. ISSN 0731-4213.

COLLEGIATE MICROCOMPUTER
Rose-Hulman Institute of Technology
Terre Haute IN 47803 USA

SUBSCRIPTION INFORMATION

CRYPTOLOGIA is a quarterly journal with issue dates of January, April, July and October. The four journals issued each year constitute one volume. The January 1983 issue is Volume 7, Number 1.

Subscription prices (U.S. Dollars): \$28.00 per year for U.S., \$36.00 per year for non-U.S. Air Mail overseas rate is \$60.00 per year. A subscription begins with the current issue as of date of receipt of request unless otherwise instructed. Back issues from January 1979, Volume 3, Number 1 to current issue are available from the Editorial Offices for \$8.00 each in the U.S. and \$10.00 each to non-U.S. address. Specify volume, number and issue date.

All orders, checks and inquiries should be sent to: CRYPTOLOGIA, Rose-Hulman Institute of Technology, Terre Haute, Indiana 47803, USA. Make checks payable to CRYPTOLOGIA.

Note to subscribers: The number in the upper right corner of your address label indicates the last issue of your subscription. The right hand (single) digit indicates the Number and the remaining left hand digit(s) indicate the Volume of the last issue in your subscription. Renew your subscription now.

CALL FOR PAPERS

CRYPTOLOGIA welcomes articles on all aspects of cryptology. We especially seek articles concerning mathematics and computer related aspects of cryptology. Articles describing new cryptosystems and methods of cryptanalysis of cryptosystems, historical articles, memoirs and translations are all sought.

Send mathematical and computer related papers to Brian J. Winkel, Division of Mathematics, Rose-Hulman Institute of Technology, Terre Haute, Indiana 47803.

Send papers, inquiries and letters concerning cryptographic machines, devices and equipment to Louis Kruh, 17 Alfred Road West, Merrick, NY 11566.

Send historical and other nontechnical articles to David Kahn, 120 Wooleys Lane, Great Neck, NY 11023.

Any paper may also be sent to the Editorial Office, CRYPTOLOGIA, Rose-Hulman Institute of Technology, Terre Haute, Indiana 47803.

Three copies should be submitted and one should be kept by the author as a protection against loss. Manuscripts should be legibly typewritten, or reproduced from typewritten copy and double-spaced with wide margins. All papers should have an Abstract and a Key-Word List after the title and author. Editorial style follows the University of Chicago Press Manual of Style. Please adhere to the footnoting style found in CRYPTOLOGIA articles. Diagrams should be done in black, suitable for off-set photo reproduction, and clearly labeled with a legend. Photographs should be clear and glossy. Indicate whether or not the photo print enclosed is to be returned.

While the ultimate responsibility for the accuracy of the material presented lies with the author(s), the Editorial Office will do its best through the refereeing and consultation process, to help insure correctness.

Authors will receive two copies of the issue in which their articles appear.

Table of Contents

A System for Verifying User Identity and Authorization at the Point-of Sale or Access	Gustavus J. Simmons	1
LUCIFER, A Cryptographic Algorithm	Arthur Sorkin	22
Reviews of Things Cryptologic	Louis Kruh and Greg Mellen	43
Who Did It?	Louis Kruh	54
Cryptanalyst's Column	Greg Mellen	55
Letters to the Editor		58
Cipher Machine Inventor - Boris Hagelin Dies	David Kahn	60
From the Archives		
- Achievements of Cipher Bureau MI-8 During the First World War	Herbert O. Yardley	62
- Because of the Freedom of Information Act	Louis Kruh	75
The Mysterious Autocryptograph	James Gillogly and Donald W. Davies	77
Biographical Sketches		93
Fourth Annual CRYPTOLOGIA Undergraduate Paper Competition		95
New Journal - COLLEGIATE MICROCOMPUTER		96

Published Quarterly at

Rose-Hulman Institute of Technology

Terre Haute, Indiana 47803 USA

CRYPTO '84

AUGUST 19-22, 1984

TO BE HELD AT
THE UNIVERSITY OF CALIFORNIA
AT SANTA BARBARA

SPONSORED BY
THE INTERNATIONAL ASSOCIATION
FOR CRYPTOLOGIC RESEARCH

ALL PERSONS INTERESTED IN THE THEORY AND APPLICATION OF CRYPTOGRAPHIC TECHNIQUES ARE INVITED AND ENCOURAGED TO ATTEND **CRYPTO '84**

PRELIMINARY CALL FOR PAPERS

PAPERS ARE SOLICITED ON ALL TOPICS RELATED TO CURRENT WORK IN THE THEORY AND APPLICATION OF CRYPTOGRAPHIC TECHNIQUES. WE WOULD ALSO LIKE TO INCLUDE A FEW HIGH-QUALITY HISTORICAL PAPERS. PLAN TO SEND SEVEN COPIES OF YOUR ABSTRACT OR COMPLETE PAPER TO: **PROF. G.R. BLAKLEY, PROGRAM CHAIRMAN**, CRYPTO '84 - DEPT. OF MATHEMATICS, TEXAS A&M UNIVERSITY, COLLEGE STATION, TEXAS 77843-3368. PHONE NO. (409) 845-7939 OR 845-3913. DEADLINE FOR PAPERS IS MAY 1, 1984. AUTHORS WILL BE NOTIFIED BY JULY 1, 1984. INFORMAL QUERIES AS TO THE SUITABILITY OF YOUR TOPIC SHOULD BE DIRECTED TO A MEMBER OF THE PROGRAM COMMITTEE.

PROGRAM COMMITTEE

G.R. BLAKLEY, CHAIRMAN (TEXAS A&M), HENRY BEKER (RACAL RESEARCH), DOROTHY DENNING (SRI INTERNATIONAL), RON RIVEST (MIT), MILES SMID (NATIONAL BUREAU OF STANDARDS).

NEW THIS YEAR — SHOW & TELL

WE WOULD LIKE TO PROVIDE AN OPPORTUNITY FOR CRYPTO '84 ATTENDEES TO SHOW AND EXPLAIN TO ONE ANOTHER CRYPTOGRAPHIC ITEMS OF CURRENT OR HISTORICAL INTEREST. IF YOU HAVE SOMETHING WHICH YOU COULD BRING TO CRYPTO '84, PLEASE CONTACT **JOE TARDO, SHOW & TELL CHAIRMAN**, CRYPTO '84 - DIGITAL EQUIPMENT CORPORATION, TWO/C11, 1925 ANDOVER STREET, TEWKSBURY, MA 01876. PHONE: (617) 858-3041. DROP HIM A NOTE NOW — WE NEED AN INDICATION OF INTEREST TO CONTINUE PLANNING FOR SHOW & TELL.

FURTHER INFORMATION

A FINAL CALL FOR PAPERS, MORE DETAILS OF THE PROGRAM, AND A REGISTRATION FORM WILL BE SENT IN THE SPRING TO ALL ATTENDEES OF PREVIOUS CRYPTO OR EUROCRYPT CONFERENCES. FOR FURTHER INFORMATION OR TO MAKE CERTAIN YOU ARE ON THE MAILING LIST, WRITE TO: **THOMAS A. BERSON, GENERAL CHAIRMAN**, CRYPTO '84 - SYTEK, INC., 1225 CHARLESTON ROAD, MOUNTAIN VIEW, CA 94043.

VOLUME 7 1983

Number 1

The Crypto '82 Conference, Santa Barbara A Report on a Conference
Cryptanalysts' Corner
Annotated Bibliography in Conventional and Public Key Cryptography
Fraternal Cryptography: Cryptographic Practices of American
Fraternal Organizations
Language Redundancy and the Unicity Point
Cryptographic Protection of Files in an Automated Office
Application of a Certain Class of Infinite Matrices to the
Hill Cryptographic System
The Power of Magic: A Book Review
Cipher Equipment: The Cryptographic Unit CSI-10
Uncaging the Hagelin Cryptograph

Number 2

A Failure of Radio Intelligence: An Episode in the Battle of the
Coral Sea
From the Archives: Account of Gen. George C. Marshall's
Request of Gov. Thomas E. Dewey
Abwehr Ciphers in Latin America
The Typex Cryptograph
Cryptanalysts' Corner
The Problem of Reciprocity in a Delastelle Digraphic Substitution
A "Weak" Privacy Protocol Using the RSA Crypto Algorithm
Remarks on a Digital Signature Scheme
The View from Across the Pond

Number 3

The Noblest Cryptologist - Duke August
An Unsolved Puzzle Solved
The Early Models of the Seimans and Halske T52 Cipher Machine
Eurocrypt 83: A Conference Report
DES-Generated Checksums for Electronic Signatures
Cryptanalysts' Corner
Book, Movie, Article and Game Reviews

Number 4

How to Use the German Enigma Cipher Machine: A Photographic Essay
The Search for the Key Book to Nicholas Trist's Book Ciphers
From the Archives: Examples of Intelligence Obtained
from Cryptanalysis
The Advent of Cryptology in the Game of Bridge
The B-21 Cryptograph
A Public-Key Cryptosystem Based Upon Equations Over Finite Field
ROTERM: A Microprocessor Based Cipher Terminal System
Cryptanalysts' Corner
Book Reviews
Index to Volume 7

CRYPTOLOGIA is a unique scholarly journal devoted to all aspects of cryptology. The journal began quarterly publication in 1977.

Areas covered include computer security, history, codes and ciphers, mathematics, military science, espionage, cipher devices, literature, and ancient languages.

Features include reviews of books and equipment, news of the crypto community, announcements of activities, challenging ciphers, and more.

CRYPTOLOGIA publishes a book on United States cryptographic patents. This is the definitive book listing and detailing over 2,000 cryptographic patents during the period 1861-1981. Richly illustrated, the work serves as a wealth of information for all cryptology enthusiasts. The book is by Dr. Jack Levine, Professor Emeritus of North Carolina State University.

ORDER BLANK FOR CRYPTOLOGIA ISSUES AND PATENT BOOK

Name _____
Address _____

[Volume 1, Nos. 1, 2, 3, 4, and Volume 2, Nos. 1, 2, 3, 4 are only available from University Microfilms, 300 North Zeeb Road, Ann Arbor MI 48106 USA.]

Volumes 3 - Current volume are available from CRYPTOLOGIA, Rose Hulman Institute of Technology, Terre Haute, IN 47803 USA.

\$8.00 each number - single and back issue price for US

\$9.00 each number - single and back issue price for non-US

CHECK material desired, total and remit check in US dollars.

Volume III	Volume IV	Volume V	Volume VI	Volume VII
No. 1	No. 1	No. 1	No. 1	No. 1
2	2	2	2	2
3	3	3	3	3
4	4	4	4	4

United States Cryptographic Patents, 1861-1981, by Dr. Jack Levine. \$10.00. [With your one year subscription - \$6.00.]

one year subscription to CRYPTOLOGIA (begin with _____)
\$28.00 (U.S.) \$36.00 (non-US) \$60.00 (non-US airmail)

AMOUNT ENCLOSED

number of back issues ordered _____
\$8.00(US) or \$9.00(non-US) Total _____

US Cryptographic Patents, 1861-1981 _____

One Year Subscription to CRYPTOLOGIA _____

Total Amount Enclosed _____

VOLUME 1 1977

Number 1

Why Cryptologia?
The Cryptology of Multiplex Systems--Part I
A Different Kind of Column
"Cracking" a Random Number Generator
The Biggest Bibliography--A Book Review
A Reply to Kahn's Review
Unity Points in Cryptanalysis
Cipher Equipment
Some Cryptographic Applications of Permutation Polynomials
Poe Challenge Cipher Finally Broken

Number 2

Age of Decipherment
"Count Forward Three Score and Ten..."
Automated Analysis of Cryptograms
Cipher Equipment
The Cryptology of Multiplex Systems--Part II
Get Out Your Secret Decoders, Boys and Girls
Analysis of the Hebern Cryptograph Using Isomorphs
Rotor Algebra
Grille Reconstruction

Number 3

The Significance of Codebreaking and Intelligence in Allied
Strategy and Tactics
The Kappa Test
Word Ways, A Journal Worth Going Your Way
Entropy Calculations and Particular Methods of Cryptanalysis
Cipher Equipment
The Earliest Use of a Dot Cipher
DPEPE DPJO
Kullback's Statistical Methods in Cryptanalysis, A Book Review
Assessment of the National Bureau of Standards Proposed Federal
Data Encryption Standard
Proposed Federal Information Processing Data Encryption Standard

Number 4

The Ithaca Connection: Computer Cryptography in the Making, A
Special Status Report
Poe Challenge Cipher Solutions
A Rapid Yes-No Computer-Aided Communicator
MA4210 Alphanumeric Pocket Cipher
Ecclesiastical Cryptography, A Review
Equivalences of Vigenere Systems
Cryptography at the Colorado School of Mines
Cryptanalysis and Data Security Course at the University of
Tennessee
Cryptanalytic Attack and Defense: Ciphertext-only, Known
Plaintext, Chosen-plaintext
Reports from the Reich
The Churchyard Ciphers
~~CENSORED~~, A Simulation Exercise
German Military Eavesdroppers
The Enigma--Part I, Historical Perspectives
There and There
Preliminary Comments on the M.I.T. Public-Key Cryptosystem
Index to Volume 1

VOLUME 2 1978

Number 1

Solving a Hagelin, Type CD-57, Cipher
Cryptanalysis Course Down Under
The Forschungsamt: Nazi Germany's Most Secret Communications
Intelligence Agency
Mathematical and Mechanical Methods in Cryptography
The Inventions of William F. Friedman
Remarks on Proposed Attack on MIT Public-Key Cryptosystem
Cryptanalysis of the Hagelin Cryptograph--A Book Review
Cryptanalyst's Corner
James Lovell and Secret Ciphers During the American Revolution
There and There

Number 2

Mathematical and Mechanical Methods in Cryptology--Part II
A Book Review--Friedman's Life, The Man Who Broke Purple
Cryptanalyst's Corner
Who Wrote The American Black Chamber?
Cryptology at Kean College
Nuggets from the Archives: Yardley Tries Again
The Unsolved D'Agapeyeff Cipher
Modern Methods for Computer Security and Privacy--A Book Review
Pictures Galore--A Book Review
Computer Methods for Decrypting Multiplex Ciphers
Casanova and the Beaufort Cipher
Cryptology as a Career
Encryption Challenge
DH-26 Handheld Encryption Unit
A Tribute to Alf Monge
There and There

Number 3

My Recollections of G.2 A.6
Computer Methods for Decrypting Random Stream Ciphers
Cryptanalysis and Computers
Cryptanalysts' Corner
A Catalog of Historical Interest
Astle Cipher Solved
A Famous Variation--A Book Review
Reveling in Deception--A Book Review
Decoding Wesley's Diaries
Short Notices--Book Reviews
Hagelin Machine (M-209) Reconstruction of Internal Settings
Capsule Reviews for Crypto Buffs
There and There

Number 4

Security of Number Theoretic Public Key Cryptosystems Against
Random Attack--Part I
What the Nazis Were Doing
The Riverbank Publications on Cryptology
Extraordinary Codebreakers, Outstanding Family--A Book Review
A 19th Century Challenge Cipher
Cryptanalysis' Corner
A Catalog of Historical Interest--Part II
An Application of Computers to Cryptography
One of the Worst--A Book Review
Rent a Code
Action Line Challenge
Data Encryption Gurus
There and There
Index to Volume 2

VOLUME 3 1979

Number 1

The Ultra Conference
How Did TJB Encode E2?
Report on the Decipherment of the American Strip Cipher 0-2
Courses in Cryptology
Security of Number Theoretic Public Key Cryptosystems Against
Random Attack--Part II
The HP-67/97 Cryptograph
A Xerograph of a Classic
Papers Disclose Allies' Edge in Knowing German Codes
A Sherlockian Cryptogram
There and There

Number 2

Early Work on Computers at Bletchley
The Hagelin Cryptographer, Type C-52
Solution of Challenge Cipher
American Codes--A Book Review
The Macbeth Test Message
Security of Number Theoretic Public Key Cryptosystems Against
Random Attack--Part III
A German Consular Cipher
Littlewood's Cipher
Ultra Goes to War--A Book Review

Number 3

The NSA Perspective on Telecommunications Protection in the
Nongovernmental Sector
J. F. Byrne and the Chaocipher - Work in Progress
Solving a Cipher Based on Multiple Random Number Streams
The Futility of It All
The Deadly Double Advertisement - Pearl Harbor Warning or
Coincidence
Littlewood's Cipher--Part II: A Method of Solution The Two-
Message Problem in Cipher Text Autokey--Part I
How to Swindle Rabin
The Second Beale Cipher Symposium - Call for Papers

Number 4

Musical Cryptography
Cryptographic Aspects of Data Compression Codes
CP-III: One Time Cypher Pad Manual Encryption Device
The Geheimschreiber
Ciphers for the Educated Man
Short Notices
The Two-Message Problem in Cipher Text Autokey--Part II
A Musical Cipher
Language Redundancy and Cryptanalysis
The Day the Friedmans Had a Typo in Their Photo
Cryptanalysis' Corner
A German Code Book
A Theory of Cryptography
There and There
Index to Volume 3

VOLUME 4 1980

Number 1

The Solution of a Cromwellian Era Spy Message
The CRYPTOMATIC HC-520
Cryptographic Reflections on the Genetic Code
A Note on Public-Key Cryptosystems
Deciphered Texts--A Book Review
Memories of Friedman
Cryptanalysts' Corner
"Forwards and Backwards" Encryption
The Ciphering System for A 19th Century Challenge Cipher
Problems of the Unbreakable Cipher
Another Solution to the Sherlockian Cryptogram
The Market for Encryption
Reminiscences of a Master Cryptograph
There and There

Number 2

Interviews with Cryptologists
Applications of the Drazin Inverse to the Hill Cryptographic
System--Part I
A Curious Cryptic Composition
Some Cryptographic and Computing Applications of the Toshiba LC-
836MN Memo Note 30 Pocket Calculator
Ready-made Love Letters
An Apology for Jacopo Silvestri
Memories of the Pacific--Book Reviews
Decryption of Simple Substitution Cyphers with Word Divisions
Using a Content Addressable Memory
The Beale Cypher: A Dissenting Opinion
Nuggets from the Archive: A Null Code at the White House
Solutions
There and There

Number 3

The Black Chamber: How the British Broke Enigma
High Speed Indirect Cryption
Finger Counting and the Identifications of James VI's Secret
Agents
Applications of the Drazin Inverse to the Hill Cryptographic
System--Part II
Opportunities for the Amateur Cryptanalyst Can Be Anywhere
Spy Ciphers--A Book Review
Cryptanalysts' Corner
Cipher Devices: TRS-80 Data Privacy System
Linear Transformations in Galois Fields and Their Applications to
Cryptography

Number 4

Some Special War Work--Part I
Remarks on Lu and Lee's Proposals for a Public-Key Cryptosystem
Cryptanalysts' Corner
Development of Commercial Cryptosystem Standards
Cipher Equipment: TST-1221
Transfinite Cryptography
Pearl Harbor Revisited--A Book Review
A Professional's Challenge
The Black Chamber: La Methodes des Batons
A Remarkable View of Ancient America--A Book Review
Results of Reader Survey
Index to Volume 4

VOLUME 5 1981

Number 1

Graphic Solution of a Linear Transformation Cipher
The Public's Secrets
Statistical Analysis of the Hagelin Cryptograph
Some Special War Work--Part II
Cryptanalysts' Corner
The Black Chamber: Shutting Off
Cipher Equipment: Collins CR-200/220
Decrypting a Stream Cipher Based on J-K Flip Flops
From the Ultra Conference--A Book Review
A Theoretical Measure of Cryptographic Performance

Number 2

German Spy Cryptograms
Applications of the Drazin Inverse to the Hill Cryptographic System--Part III
The Code-O-Graph Cipher Disks
The House Report on Public Cryptography
The Hand-Held Calculator as a Cryptographic Machine
The Public Cryptography Study Group
Cryptanalysts' Corner
A Code Problem--A Book Review

Number 3

Report of the Public Cryptography Study Group
The Case against Restraints on Non-Governmental Research in Cryptography
Announcement: Undergraduate paper Competition in Cryptology
Palatine and Bibliander on Ciphers
Reward for Reading and Deciphering--A Book Review
Measuring Cryptographic Performance with Production Processes
Sherlock Holmes in Babylon
Cipher Machine Exhibit at the Smithsonian Institution
The A-22 Cryptograph
There and There

Number 4

The Genesis of the Jefferson/Bazeries Cipher Devices
A User's Guide in Voice and Data Communications Protection--A Book Review
Letters to the Editor
Applications of the Drazin Inverse to the Hill Cryptographic System--Part IV
Secret Writing Exhibit
Higher-Order Homophonic Ciphers
Number Theory in Digital Signal Processing--A Book Review
Interactive Solution of Columnar Transposition Ciphers
Index to Volume 5

VOLUME 6 1982

Number 1

Mathematical Solution of the Enigma Cipher
In Memoriam: Marian Rejewski
Why Germany Lost the Code War
Enigma Solved
The Black Chamber
Wilderness of Mirrors--A Book Review
Beale Society Material--A Book Review
If I Remember
Cryptanalysts' Corner
Churchill Pleads for the Intercepts
A Conversation with Marian Rejewski
Unraveling the Enigma Story--A Book Review
From the Depths to the Heights--Book Reviews
Remarks on Appendix 1 to British Intelligence in the Second World War by F. H. Hinsley
Computer Cryptography--A Book Review
The Navy Cipher Box Mark II

Number 2

Use of Microcomputer System for Medical Record Encryption and Decryption Using a Sequential Pseudo-Random Key
The Performance of Hellman's Time Trade-Off against Rotor Cipher
A New Source for Historians: Yardley's Seized Manuscripts
In Memoriam: Georges-Jean Painvin
Error-Correcting Codes and Cryptography--Part I
Book Reviews
Cryptanalysts' Corner
Konheim's Cryptography--A Primer--A Book Review
Sirius
There and There
Announcement of Second Annual Undergraduate Paper Competition

Number 3

Rhapsody in Purple, a New History of Pearl Harbor--Part I
Factoring Via Superencryption
The Mystery of Colonel Decius Wadsworth's Cipher Device
Cryptanalysts' Corner
Cryptographic Features of the UNIX Operating System
Error-Correcting Codes and Cryptography--Part II
Ciphertext Only Attack on the Merkel-Hellman Public-Key System under Broadcast Situations
Solution to Sirius Music Cipher
Helmich and the KL-7

Number 4

The Siemens and Halske T52e Cipher Machine
Cryptanalysts' Corner
Applications of Vincent's Theorem in Cryptography
Breaking a Pseudo Random Number Based Cryptographic Algorithm
Digital Signature Schemes
A Pedagogical Cipher
Rhapsody in Purple, A New History of Pearl Harbor--Part II
A Child's Garden of Cryptography
A Basic Probe of the Beale Cipher as a Bamboozlement
Index to Volume 6